VigiLife Information Security Policies, Controls and Procedures

Security Program Overview

2024.04.01

VigiLife is committed to protecting its employees, partners, clients/customers and the company itself from damaging acts either malicious or unintentional in nature. This includes implementation of policies, standards, controls and procedures to ensure the Confidentiality, Integrity, and Availability of systems and data according to their risk level.

The VigiLife security program and policies are developed on the principles that (1) security is everyone's responsibility and (2) self-management is best encouraged by rewarding the right behaviors.

Reference Employee Handbook for summarized items employees should be mindful of.

Sections

Information Security Program and Scope

VigiLife has developed a security program and implemented controls to meet and exceed all compliance requirements, including but not limited to HIPAA,

NIST, SOC 2 Common Criteria and other applicable industry best practices.

On a high level, VigiLife's information security program covers:

1. Inventory and protection of all critical assets
2. Visibility into and the management of data lifecycle, from creation to retention to deletion
3. Protection of data-at-rest, data-in-transit, and data-in-use
4. Segmented network architecture
5. Automated security configuration and remediation
6. Centralized identity and access management
7. Secure product development
8. Continuous monitoring and auditing
9. Validated plan and practice for business continuity, disaster recovery, and emergency response
10. End-user computing protection and awareness training

More information about the VigiLife Security and Privacy program can be found at https://www.vigilife.com/security and https://www.vigilife.com/privacy.

The information security program and its policies and procedures cover all VigiLife workforce members, including full-time and part-time employees in all job roles, temporary staff, contractors and subcontractors, volunteers, interns, managers, executives employees, and third parties.

The information security program is managed by dedicated security and compliance personnel, using as a GRC platform.

Understanding the Policies and Documents

Policies are written in individual documents, each pertaining to a specific domain of concern.

Each document starts with the current version number and/or last updated date, followed by a brief summary. The remaining of the document is structured to contain two main sections:

- Policy Statements
- Controls and Procedures

All policy documents are maintained, reviewed, updated and approved following standards and procedures outlined in Policy Management.

Review and Reporting

The information security program, policies, procedures and controls are reviewed on a regular basis internally by cross functional team members and externally by qualified assessors.

Corporate Governance

2024.02.13

VigiLife believes in transparent and ethical business practices, and the protection of long-term interests of its employees, customers, shareholders and other stakeholders.

VigiLife has established a Board of Directors (Bod) and appointed qualified members and directors, such that:

- A corporate bylaws and BoD charters are in place that describe board members responsibilities.
- The BoD identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- Board members are evaluated on a periodic basis to help ensure their skills and expertise are suited to lead senior management and take commensurate action.
- The BoD has sufficient members who are independent from management and are objective in evaluations and decision making.
- The expectations of the BoD and/or senior management are defined and understood at all levels of the organization and its service providers and business partners.

Controls & Procedures

Board of Directors Responsibilities

The Board of Directors (BoD) meets quarterly to discuss financials, operations, business results, strategies and planning. The BoD responsibilities include:

- Evaluate the performance of the Chief Executive Officer (CEO) and the executive management team
- Establish policies, evaluate and approve the compensation of senior management of the company
- Review succession plans and development programs for senior management
- Review and approve long-term strategic and business plans and monitor organization's performance against the plans
- Review and approve any major risks and the risk remediation/acceptance
- Adopt policies of corporate conduct, including compliance with applicable laws, rules and regulations, maintenance of accounting, financial and other controls, and reviewing the adequacy of compliance systems and controls
- Evaluate the overall effectiveness of the Board and its committees and the individual directors on a periodic basis
- Adopt and implement best practices of corporate governance in full conformity with the letter and spirit of all applicable laws, rules and regulations

Policy Management

2024.02.13

VigiLife implements policies and procedures to maintain compliance and integrity of data. The Security Officer and Privacy Officer are responsible for maintaining policies and procedures and assuring all VigiLife workforce members, business associates, customers, and partners are adherent to all applicable policies. Previous versions of policies are retained to assure ease of finding policies at specific historic dates in time.

Policy Statements

VigiLife policy requires that:

(a) VigiLife policies must be developed and maintained to meet all applicable compliance requirements adhere to security best practices, including but not limited to:

- HIPAA
- NIST
- SOC 2

(b) All policies must be reviewed at least annually.

(c) All policy changes must be approved by VigiLife Security Officer. Additionally,

- Major changes may require approval by VigiLife CEO or designee;

- Changes to policies and procedures related to product development may require approval by the Head of Engineering.

(d) All policy documents must be maintained with version control, and previous versions must be retained for a defined, predetermined timeframe.

(e) Policy exceptions are handled on a case-by-case basis.

- All exceptions must be fully documented with business purpose and reasons why the policy requirement cannot be met.
- All policy exceptions must be approved by both VigiLife Security Officer and COO.
- An exception must have an expiration date no longer than one year from date of exception approval and it must be reviewed and re-evaluated on or before the expiration date.

Controls & Procedures

Policies and Controls Framework

VigiLife maintains a set of policies and controls that captures standards, regulatory, legal, and statutory requirements relevant to the business needs. The framework and its contents are reviewed at least annually to ensure changes that could affect the business processes are reflected.

Structure

Similar to the concept of "micro-services", the policies and control procedures are written in individual "micro-docs". They are mapped to each other via a JSON configuration.

Controls Mapping

A JSON document configures the mapping of each control procedure to one or more security/compliance frameworks, as applicable.

Note that the controls mapping is only between a control/procedure document to the requirement, not at the policy level. This is because we strongly believe that you must have documented controls and procedures to implement and enforce a high level written policy. Having a written policy by itself without implementation or enforcement does not address the risk of any security or compliance requirement.

Compliance standards

At least once a year, VigiLife reviews the regulatory, legal, and statutory requirements relevant to its business needs and adopts any relevant standards into its controls framework and governance program.

The list of applicable standards can be found it the same repository as the policies and controls documentation and/or in the compliance management application/platform.

Policy Management Process

Document Structure

Policies are written in individual documents, each pertaining to a specific domain of concern.

Each document starts with the current version number in the format of YYYY.# (e.g. 2017.1), followed by a brief summary. The remaining of the document is structured to contain the following subsections:

- Policy Statements
- Applicable Standards
- Controls and Procedures

Versioning

Each VigiLife policy document contains a version and optionally a revision number. The version number is the four digit year followed by a number, to indicate the year and sequence number of the policy at which time it was written or updated.

The version number shall be incremented by one with each material change to the policy content. For example, if a new policy statement is added or a technical control/procedure is updated to 2017.1 version of a policy, the new version should be numbered 2017.2.

The policy document may also include a revision number, in the format of rev.#, immediately following the main version number. A revision number indicate minor, non-material changes to the document, such as formatting changes, fixing typos, or adding minor details.

Numbering

If sequencing numbers are included in the policy headings:

- Policy may be referenced by its statement number, such as §2.1(a), in internal/external communications as well as in other VigiLife policies or technical/business documentation for cross reference.

- As such, to maintain cross referencing integrity, starting from version 2017.2, all numbering shall remain intact for policy documents and statements.
- When updating, avoid reordering and renumbering of policy documents and statements. For example:
    - Append at the end of the list by adding new statement(s) as needed instead of inserting.
    - If a policy or policy statement is no longer applicable, mark it deprecated instead of removing the file or statement completely.

Review and Maintenance of Policies

1. All policies are stored and up to date to maintain VigiLife compliance with HIPAA,

   NIST, SOC 2 and other relevant standards. Updates and version control are done similar to source code control.

2. Policy update requests can be made by any workforce member at any time. Furthermore, all policies are reviewed annually by the Security and Privacy Officer to assure they are accurate and up-to-date.

3. VigiLife employees may request changes to policies using the following process:

    1. The VigiLife employee initiates a policy change request by creating an Issue in the GitHub Issues Security project. The change request may optionally include a GitHub pull request from a separate branch or repository containing the desired changes.

    2. The Security Officer or the Privacy Officer is assigned to review the policy change request.

    3. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

    4. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

    5. If the policy change requires technical modifications to production systems, those changes are carried out by authorized personnel using VigiLife's change management process.

    6. If the change results in a new version instead of a new revision (see §3.3.1 for definitions), the current version of the policy document(s) must be saved to archive under the corresponding version number prior to the new policy being adopted/published and prior to merging the pull request containing the changes. This allows easy reference to previous versions if necessary.

Important

* Changes are made on the `drafts` (or equivalent) branch instead of on the `master` branch for commits.
* If multiple authors are working on the changes, additional separate branches and pull requests may be necessary before changes are merged in `drafts`.
* Changes must not be merged to `master` without the approval of Security and Privacy Officer.
* Changes must not be merged to `master` without archiving the existing version of policy document(s), unless the change is a minor revision.
* Once the changes are final and approved, a pull request shall be created from the `drafts` branch to the `master` branch and all members of the development team shall be included as app
* Policy update communication and training for non-development staff is conducted separately by the Security team.

4. All policies are made accessible to all VigiLife workforce members. The current master policies are published at https://www.vigilife.com/security.

* Changes are automatically communicated to all VigiLife team members
  through integrations between GitHub and Slack that log changes
  to a predefined VigiLife Slack Channel.
* The Security Officer also communicates policy changes to all employees via
  email. These emails include a high-level description of the policy change
  using terminology appropriate for the target audience.

5. All policies, and associated documentation, are retained for 7 years from the date of its creation or the date when it last was in effect, whichever is later

1. Version history of all VigiLife policies is done via GitHub.
2. Backup storage of all policies is done with AWS S3 and/or internal file
   share (e.g. Microsoft Office365 SharePoint or Box).

6. The policies and information security policies are reviewed and audited annually, or after significant changes occur to VigiLife's organizational environment, by the security committee members. Issues that come up as part of this process are reviewed by VigiLife management to assure all risks and potential gaps are mitigated and/or fully addressed. The process for reviewing polices is outlined below:

1. The Security Officer initiates the policy review by creating an Issue in
   the GitHub Issues Security project or via a Pull Request (PR).
2. The Security Committee members and additional reviewers are notified by
   email or via the PR to review the current policies.
3. If changes are made, the above process is used. All changes are
   documented in the Issue/PR.
4. Once the review is completed, the Security Officer approves or rejects
   the Issue/PR. If the Issue/PR is rejected, it goes back for further
   review and documentation.
5. If the review is approved, the Security Officer then marks the Issue as
   Done, or merges the PR into master branch, adding any pertinent notes
   required.
6. Policy review is monitored using GitHub Issues or GitHub
   reporting to assess compliance with above policy.

Additional documentation related to maintenance of policies is outlined in Roles and Responsibilities.

Security Architecture and Operating Model

2024.02.13

In the digital age, cyber attacks are inevitable. At VigiLife, we are taking a “zero trust”, “minimal infrastructure” approach to managing risk and information security.

This document describes our guiding principles and aspirations in managing risk and the building blocks of our security model.

Policy Statements

VigiLife policy requires that:

(a) VigiLife's security program and operations should be designed and implemented with the following objectives and best practices:

- data-centric, cloud-first
- assume compromise therefore never trust, always verify
- apply controls using least-privilege and defense-in-depth principles
- avoid single point of compromise
- automate whenever possible, the simpler the better, less is more
- prompt self management and reward good behaviors

(b) Security shall remain a top priority in all aspects of VigiLife's business operations and product development.

Controls & Procedures

VigiLife Security Principles
(1) Data-centric model; zero-trust architecture

“Zero Trust” is a data-centric security design that puts micro-perimeters around specific data or assets so that more granular rules can be enforced. It remedies the deficiencies with perimeter-centric strategies and the legacy devices and technologies used to implement them. It does this by promoting “never trust, always verify” as its guiding principle. This differs substantially from conventional security models which operate on the basis of “trust but verify.”

In particular, with Zero Trust there is no default trust for any entity — including users, devices, applications, and packets—regardless of what it is and its location on or relative to the corporate network. In addition, verifying that authorized entities are always doing only what they’re allowed to do is no longer optional; it’s now mandatory.

Summary

* No internal network. (Almost) 100% cloud.
* Fully segregated with Granular policy enforcements.
* Individually secured devices. No production access by default.

(2) “Air-Gapped” environments meet short-lived processes

We extend the zero-trust security model with a “Minimal Infrastructure” approach, where we use “Anything-as-a-Service” whenever possible, to harness the full power of the cloud. Cloud services allow us to contain and control access at a much more granular level, compared to operating on-premise infrastructure. Via access to the extensive APIs provided by the cloud services, we would be able to more easily integrate and automate security operations. Additionally, minimizing infrastructure significantly reduces always-on attack surfaces. Services that are not used are turned off, instead of being idly available which opens itself up to attacks. Together with Zero Trust, this security model and architecture enables a high degree of flexibility for end-user computing while maintaining the highest level of security assurance.

Summary

* Processes are short-lived and killed after use.
* Minimal persistent attack surface making it virtually impenetrable.

(3) Least-privilege temporary access

Cyber attacks are inevitable. When it comes to preparing for potential attacks, VigiLife security operations take the approach that assumes a compromise can happen at any time, to any device, with little to no indicators. This is also an extension of the “zero trust” model. When building security operations, we carefully perform risk analysis and threat model, to identify potential single point of compromise.

In other words, compromise of any single system or user or credential, should not easily lead to a broad or full compromise of the entire infrastructure or operations. For example, if an attacker gains access to a admin credential (e.g. Active Directory domain), it should not directly lead to the compromise of all systems and data in the environment.

Summary

* Need-based access control for both employees and computing services.

* Access to critical systems and resources are closed by default, granted on demand.
* Protected by strong multi-factor authentication.
* No single points of compromise.
* "Secrets" (such as SSH Keys) must remain secret at all times.

(4) Immutable builds and deploys

The VigiLife platform leverages a micro-service architecture. This means that the system has been decomposed into numerous small components that can be built and deployed individually. Before these components get deployed to our *production* environments, we thoroughly test and validate the changes in our *lower* environments which are completely isolated from production. This allows us to test upcoming changes while ensuring there is no impact to our customers.

As a particular build of a component progresses through our environments, it is important that the build does not change thus we ensure that each build is immutable. Once an *immutable build* has been validated in our *lower* (non-production) environments, we then deploy it to our *production* environment where the change will be available to VigiLife customers and end-users.

Changes to our infrastructure (database schema changes, storage buckets, load balances, DNS entries, etc.) are also described in our source code and deployed to our environments just like the applications. This architectural approach to managing infrastructure is referred to as *infrastructure as code* and is a key requirement for fully automated deployments with minimal human touch.

Summary

* Infrastructure as code with active protection.
* Automated security scans and full traceability from code commit to production.
* “Hands-free” deployment ensures each build is free from human error or malicious contamination.

(5) End-to-end data protection and privacy

It is of the utmost importance that VigiLife provides for confidentiality (privacy), integrity and availability of its customer's data. Your data is protected with encryption in transit and at rest, combined with strong access control and key management. We will never use or share your data without your prior consent.

Summary

* Data is safe both at rest and in transit, using strong encryption, access control and key management.
* Data is not shared without prior consent

(6) Strong yet flexible user access

We all know by now that "Passw0rd" makes a terrible password. Access control is so important we must get it right. That's why we leverage tried-and-true technology such as SAML, OAuth, multi-factor authentication, and fine-grained authorization to provide strong yet intuitive access options, both for our internal staff to access business resources and for our customers to access VigiLife platform and services.

Summary

* OAuth 2.0, OpenID Connect, SAML for customer authentication and single sign-on.
* Multi-factor authentication.
* Fine-grain attribute-based or role-based authorization.

(7) Watch everything, even the watchers

You can’t protect what you can’t see.

As the famous strategist, Sun Tzu, once said, “Know thy self, know thy enemy. A thousand battles, a thousand victories.” It all starts with knowing ourselves. This applies to the infrastructure, environments, operations, users, systems, resources, and most importantly, data. It is important to inventory all assets, document all operations, identify all weaknesses, and visualize/understand all events.

This includes conducting various risk analysis, threat modeling, vulnerability assessments, application scanning, and penetration testing. Not only that, this requires security operations to keep an eye on everything, and someone should also "watch the watchers".

At first, this would require significant manual effort and may seem impossible to keep up-to-date. Our goal is to automate security operations, so that this can be achieved programmatically as our operations evolve to become more complex.

Additionally, VigiLife security team will actively monitor threat intelligence in the community, with feeds and information sharing platform such as NH-ISAC to stay abreast of the attacker activities and methodologies.

Summary

* Environments are monitored; Events are logged; Alerts are analyzed; Assets are tracked.
* No privileged access without prior approval or full auditing.
* We deploy monitoring redundancy to “watch the watchers”.

(8) Centralized and automated operations

As much as possible, VigiLife security will translate policy and compliance requirements into reusable code for easy implementation and maintenance. This allows us to truly be able to enforce policy and compliance in a fast and scalable way, rather than relying solely on written policies and intermittent manual audits.

Automation makes it truly possible to centralize security operations, including not only event aggregation and correlation, but also the

orchestration and management of previously siloed security controls and remediation efforts.

Summary

* API-driven cloud-native security fabric that
  - centrally monitors security events,
  - visualizes risk management,
  - automates compliance audits, and
  - orchestrates near real-time remediation.

(9) Usable security

Security benefits from transparency, and should operate as an open-book. This allows the entire organization to take responsibility for and accountability of adopting security best practices. Similar to code reviews and pull requests in the development process, VigiLife security team makes security standards and practices available to all employees for feedback prior to adoption.

We emphasize on the usability and practicality of security. A security solution or process is not effective, if it is not being used, no matter how good it may be. Having impractical security would only generate noise, provide a false sense of security, and incur unnecessary cost. Nothing is perfect, but we embrace an agile mindset to test and try, and to continuously improve.

Summary

* All employees receive security awareness training annually
* Simple policies, processes, and procedures.
* No “Shadow IT”.
* Processes that encourage self management and reward good behavior.

(10) Regulatory compliant

Security != Compliance. We cannot have one without the other.

Summary

* Regulatory Compliant;
* Independently assessed and certified;

Security Architecture

VigiLife has developed a security architecture on top of its three main infrastructure environments - Cloud (AWS), DevOps, and workforce collaboration / end-user computing.

Architecture Diagrams

Detailed architecture diagrams of the in-scope networks, endpoints, applications as well as the security operations are developed and maintained by .

Cloud Architecture
Cloud Native

- Designed for the cloud using true multi-tenant architecture
- Auto scaling using Serverless architecture
- Infrastructure as Code
- Ongoing security monitoring and evaluation using cloud services

Customer Benefits

- Infrastructure is tailored to our customer's goals and usage patterns
- "Shared use" model reduces cost
- Nearly infinite compute and data capacity via AWS cloud provider
- Customers can focus on solving business problems and not worry about infrastructure
- Automatic backup and recovery
- Continuous improvements via change control process
- Faster adoption of new technology

Evolution of Cloud Computing

1. Baremetal
    - A computer in someone else's data center
2. Virtual Machine
    - A portion of a computer in someone else's data center
    - In AWS, a Virtual Machine is created from Amazon Machine Image (AMI)
3. Container
    - A package of essential application libraries and code but not the core OS libraries - Simpler to scale a docker image because - No duplication of core OS processes (networking, filesystem, etc) - Typically a Docker container
4. Function

    - Just the application code that runs in a pre-built container

VigiLife strives to leverage functions as the primary building blocks for our platform because:

- functions deploy more quickly than containers and virtual machines
- functions limit the blast radius of an indicent
- AWS automatically scales Lambda functions based on the number of incoming invocations
- they are short-lived processes which minimizes attack surface

Metrics, Measurements and Continuous Monitoring

A set of metrics / KPIs have been defined to assist in the measuring, reporting and optimizing the security program and the controls in place.

A security scorecard is produced every with updates to key metrics of the VigiLife information security program, to measure its adoption and effectiveness.

The reports and scorecards are maintained by and can be accessed at .

Quality of Service

VigiLife strives to provide a high quality of service to all of its customers. This is accomplished through a security architecture that encompasses all of VigiLife's operations and provides high data confidentiality, integrity, and availability.

An overview of VigiLife's architecture can be found in Security Architecture. VigiLife uses a highly scalable cloud architecture to provide system quality at all times.

All systems are monitored and measured in real time as described in Application Service Event Recovery.

VigiLife uses DevOps methodology as described in Software Development Process to ensure a smooth delivery process of all systems and applications.

Status for external facing, customer applications and systems is published at .

Roles, Responsibilities and Training

2024.04.02

Security and compliance is everyone's responsibility. VigiLife is committed to ensuring all workforce members actively address security and compliance in their roles. Statistically, cybersecurity breaches typically start with compromise of end-user computing devices, social engineering, human error or insider threat. Therefore, users are the first line of defense and yet usually the weakest link. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

In this and all related policy documents, the term "employees" and "workforce members" may be used interchangeably to include all full-time and part-time employees in all job roles, contractors and subcontractors, volunteers, interns, managers and executives at VigiLife.

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, testing, implementation, training, and oversight of all activities pertaining to VigiLife's efforts to be compliant with the applicable security and compliance regulations and industry best practices. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of critical and sensitive data. The Security and Privacy Officer is appointed by and reports to the Board of Directors and/or the CEO.

VigiLife has appointed Robert Ficcaglia as the Security Officer and Mats Nahlinder as the Privacy Officer.

An official **Security Team** has been formed, chaired by the Security Officer, and represented by the select members of the senior leadership team (CEO, VP of Engineering, VP of Product & Partnerships, VP of Security).

Policy Statements

VigiLife policy requires that:

(a) A Security and Privacy Officer [164.308(a)(2)] must be appointed to assist in maintaining and enforcing safeguards towards security, compliance, and privacy.

(b) Security and compliance is the responsibility of all workforce members (including employees, contractors, interns, and managers/executives). All workforce members are required to:

- Complete all required security trainings, including annual regulatory compliance training, security awareness, and any additional role-based security training as part of the ongoing security awareness program and as required by job role.
- Complete annual HIPAA awareness training
- Follow all security requirements set forth in VigiLife security policy and procedures, including but is not limited to access control policies and procedures and acceptable use policy for end-user computing.
- See something, say something: follow the incident reporting procedure to report all suspicious activities to the security team.

(c) All workforce members are required to report non-compliance of VigiLife's policies and procedures to the Security Officer or designee. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

(d) All workforce members are required to cooperate with federal, state and local law enforcement activities and legal investigations. It is strictly prohibited to interfere with investigations through willful misrepresentation, omission of facts, or by the use of threats against any person.

(e) Workforce members found to be in violation of this policy will be subject to sanctions.

(f) Segregation of Duties shall be maintained when applicable to ensure proper checks and balances and minimize conflict of interests. This helps reduces the possibility of fraud and insider threat considerably, and eliminates single points of compromise to critical systems.

Controls & Procedures

Assignment of Roles and the Security Team

VigiLife has appointed Robert Ficcaglia as the Security Officer and Mats Nahlinder as the Privacy Officer.

The security team is chaired by the Security Officer, and represented by the select members of the senior leadership team, including CEO, VP of Engineering, VP of Product & Partnerships, VP of Security, in addition to the Security and Privacy Officer.

General Responsibilities of the Security and Privacy Officer

The authority and accountability for VigiLife's information security program and privacy program is delegated to the Security and Privacy Officer. The Security Officer and the security team are required to perform or delegate the following responsibilities:

- Build and maintain security and privacy program to satisfy regulatory and contractual requirements.
- Establish, document, distribute and update security policies, standards and procedures.
- Oversee, enforce and document all activities necessary to maintain compliance and verifies the activities are in alignment with the requirements;
- Monitor, analyze, distribute and escalate security alerts and information.
- Develop and maintain security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to critical systems and data.
- Perform risk assessment, remediation, and ongoing risk management.
- Provide regular security awareness and compliance training, as well as periodic security updates and reminder communications for all workforce members.
- Maintains a program that incentivizes right behaviors, supports timely and proper reporting and investigation of violations, implements effective and practical mitigation, and applies fair sanctions when necessary.
- Assist in the administration and oversight of business associate agreements.
- Facilitate audits to validate compliance efforts throughout the organization.
- Work with the COO/CFO to ensure that any security objectives have appropriate consideration during the budgeting process.

Workforce Supervision Responsibilities

Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining compliance, it is everyone's responsibility (i.e. team leaders, supervisors, managers, co-workers, etc.) to supervise all workforce members and any other user of VigiLife's systems, applications, servers, workstations, etc. that contain sensitive data.

1. Monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
2. Assist the Security and Privacy Officers to ensure appropriate role-based access is provided to all users.
3. Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and VigiLife's security policies and procedures.

Segregation of Duties

VigiLife has dedicated team/personnel assigned the job function of security and compliance. Segregation of duties are achieved via a combination of assignment of roles and responsibilities to different personnel, and automation enforcement for software-defined processes.

Checks and balances are ensured via such segregation of duties and related review/approval processes. When applicable, reviews and approvals must be obtained from designated personnel separate from the individual performing the work.

Policy and Compliance Training

1. The Security & Privacy Officer facilitates the training of all workforce members as follows:
    1. New workforce members within their first month of employment;
    2. Existing workforce members annually;
    3. Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;
    4. Existing workforce members as needed due to changes in security and risk posture of VigiLife.
2. Documentation of the training session materials and attendees is retained for a minimum of seven years.
3. The training session focuses on, but is not limited to, the following subjects defined in VigiLife's security policies and procedures:
    1. SOC 2 Security Principals and Controls;
    2. NIST Security Rules;
    3. HIPAA Privacy, Security, and Breach notification rules;
    4. Risk Management procedures and documentation;
    5. Auditing. VigiLife may monitor access and activities of all users;
    6. Workstations may only be used to perform assigned job responsibilities;
    7. Users may not download software onto VigiLife's workstations and/or systems without prior approval from the Security Officer;
    8. Users are required to report malicious software to the Security Officer immediately;
    9. Users are required to report unauthorized attempts, uses of, and theft of VigiLife's systems and/or workstations;
    10. Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation);
    11. Users may not alter sensitive data maintained in a database, unless authorized to do so by a VigiLife Customer;
    12. Users are required to understand their role in VigiLife's contingency plan;
    13. Users may not share their user names nor passwords with anyone;
    14. Requirements for users to create and change passwords;
    15. Users must set all applications that contain or transmit sensitive data to automatically log off after 15 minutes of inactivity;
    16. Supervisors are required to report terminations of workforce members and other outside users;
    17. Supervisors are required to report a change in a users title, role, department, and/or location;
    18. Procedures to backup sensitive data;
    19. Procedures to move and record movement of hardware and electronic media containing sensitive data;
    20. Procedures to dispose of discs, hard drives, and other media containing sensitive data;
    21. Procedures to re-use electronic media containing sensitive data;
    22. Secrets management (such as SSH key) and sensitive document encryption procedures.

Ongoing Awareness Training

VigiLife leverages to deliver innovative, fun and engaging security awareness contents to all employees yearly. This security awareness training shall include modules on

- phishing,
- social engineering,
- proper internet use (social media, email, clicking, etc),
- access control (proper passwords, 2FA, screen locking, etc),
- mobile device security,
- data protection, and
- system security (anti-malware, patches, secure configuration, etc).

Progress is tracked individually for each employee and reported on 's cloud-managed learning platform.

HIPAA Awareness Training

VigiLife requires all employees to take a HIPAA awareness training within 30 days of onboarding and annually thereafter. The training record is captured within the HR record and/or the learning system .

Internal Business Communications

Company-wide updates

VigiLife holds a company-wide roundtable at least quarterly to communicate updates across all aspects of business operations, performance and objectives.

Senior management sends out additional company-wide announcements as appropriate through pre-established internal communication channels such as email or messaging (e.g. Slack #general channel).

Departmental, team and/or project status updates

Regular performance and status updates are communicated by each department, functional team, and/or designated individuals through pre-established channels.

Additionally, each project team maintains team updates at their own committed cadence and channel -- for example, daily development standups/scrum or weekly team meetings.

Risk Management

2024.02.13

This policy establishes the scope, objectives, and procedures of VigiLife's information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

Policy Statements

VigiLife policy requires that:

(a) A thorough risk assessment must be conducted to evaluate the potential threats and vulnerabilities to the confidentiality, integrity, and availability of sensitive, confidential and proprietary electronic information it stores, transmits, and/or processes.

(b) Risk assessments must be performed with any major change to VigiLife's business or technical operations and/or supporting infrastructure, no less than once per year.

(c) Strategies shall be developed to mitigate or accept the risks identified in the risk assessment process.

(d) Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of seven years.

Controls & Procedures

Risk Management Objectives

VigiLife has established formal risk analysis and risk management processes to

- identify risks that may impact its business operations or the confidentiality, integrity and availability of its critical data; and
- reduce risk to an acceptable level by implementation of mitigation controls.

Unmitigated risk above the pre-defined acceptable level must be reviewed, approved and accepted by senior management.

Acceptable Risk Levels

Risks that are either low impact or low probability, based on the scoring mechanism defined in risk assessment process, are generally considered acceptable.

All other risks must be individually reviewed and managed according to the risk management process.

Risk Management Process

Risk analysis and risk management are recognized as important components of VigiLife's corporate compliance and information security program.

VigiLife's risk management process is developed in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).

Risk assessments are done throughout product life cycles:

- Before the integration of new system technologies and before changes are made to VigiLife physical and technical safeguards; and (Note that these changes do not include routine updates to existing systems, deployments of new systems created based on previously configured systems, deployments of new Customers, or new code developed for operations and management of the VigiLife Platform)
- While making changes to VigiLife physical equipment and facilities that introduce new, untested configurations.

VigiLife performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of sensitive data.

VigiLife implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all sensitive data VigiLife receives, maintains, processes, and/or transmits for its Customers;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of Customer data and/or sensitive data;
3. Protect against any reasonably anticipated uses or disclosures of Customer data and/or sensitive data that are not permitted or required; and
4. Ensure compliance by all workforce members.

In addition, VigiLife risk management process requires that:

1. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management and VigiLife's Security Officer.
2. All VigiLife workforce members are expected to fully cooperate with all persons charged with doing risk management work, including contractors and audit personnel. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation, as outlined in the VigiLife Roles Policy.
3. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of VigiLife's Security Officer (or other designated employee), and the identified Risk Management Team.
4. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.
5. The details of the Risk Management Process, including risk assessment, discovery, and mitigation, are outlined in detail below. The process is tracked, measured, and monitored using the following procedures:
    1. The Security Officer or the Privacy Officer initiates the Risk Management Procedures by creating an Issue in the GitHub Issues Security Project.
    2. The Security Officer or the Privacy Officer is assigned to carry out the Risk Management Procedures.
    3. All findings are documented and linked to the Issue.
    4. Once the Risk Assessment steps are complete, along with corresponding documentation, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
    5. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
6. The Risk Management Procedure is monitored on a quarterly basis using GitHub Issues reporting to assess compliance with above policy.

Third party risk management details including procurement and systems acquisition can be found in Vendor Risk Assement.

Risk Management Schedule

The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of VigiLife's information security program:

- Scheduled Basis - an overall risk assessment of VigiLife's information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
- Throughout a System's Development Life Cycle - from the time that a need for a new, untested information system configuration and/or application is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
- As Needed - the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect VigiLife's Platform.

Risk Assessment and Analysis

The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

- Step 1. System Characterization
    - The first step in assessing risk is to define the scope of the effort. To do this, identify where sensitive data is received, maintained, processed, or transmitted. Using information-gathering techniques, the VigiLife Platform boundaries are identified.
    - Output - Characterization of the VigiLife Platform system assessed, a good picture of the Platform environment, and delineation of Platform boundaries.

- Step 2. Threat Identification
    - Potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. All potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
    - Output - A threat list containing a list of threat-sources that could exploit Platform vulnerabilities.
- Step 3. Vulnerability Identification
    - Develop a list of technical and non-technical Platform vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
    - Output - A list of the Platform vulnerabilities (observations) that could be exercised by potential threat-sources.
- Step 4. Control Analysis
    - Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by VigiLife to minimize or eliminate the likelihood / probability of a threat-source exploiting a Platform vulnerability.
    - Output - List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the Platform to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
- Step 5. Likelihood Determination
    - Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
    - Output - Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 6. Impact Analysis
    - Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to VigiLife's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
    - Output - Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 7. Risk Determination
    - Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
    - Output - Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 8. Control Recommendations
    - Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
    - Output - Recommendation of control(s) and alternative solutions to mitigate risk.
- Step 9. Results Documentation
    - Results of the risk assessment are documented in an official report, spreadsheet, or briefing and provided to senior management to make decisions on policy, procedure, budget, and Platform operational and management changes.
    - Output - A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

Risk Mitigation and Monitoring

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process to ensure the confidentiality, integrity and availability of VigiLife Platform data. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

- Step 1. Prioritize Actions
    - Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list

getting/requiring the most immediate attention and top priority in allocating resources

    - Output - Actions ranked from high to low

- Step 2. Evaluate Recommended Control Options

    - Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.

    - Output - list of feasible controls

- Step 3. Conduct Cost-Benefit Analysis

    - Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.

    - Output - Documented cost-benefit analysis of either implementing or not implementing each specific control

- Step 4. Select Control(s)

    - Taking into account the information and results from previous steps, VigiLife's mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to data confidentiality, integrity, and availability. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

    - Output - Selected control(s)

- Step 5. Assign Responsibility

    - Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

    - Output - List of resources, responsible persons and their assignments

- Step 6. Develop Safeguard Implementation Plan

    - Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:

        - Each risk or vulnerability/threat pair and risk level;
        - Prioritized actions;
        - The recommended feasible control(s) for each identified risk;
        - Required resources for implementation of selected controls;
        - Team member responsible for implementation of each control;
        - Start date for implementation
        - Target date for completion of implementation;
        - Maintenance requirements.

    - The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to VigiLife Senior Management.

    - Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframe and expectations. Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.

    - Output - Safeguard Implementation Plan

- Step 7. Implement Selected Controls

    - As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.

    - Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

    - Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.

    - If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

    - Output - Residual Risk documentation

Risk Registry

VigiLife Security team maintains a registry of risks, captured and kept updated

- in a document on company SharePoint; and/or
- in the security operations tool/database.

The risk registry includes all risks and threats identified during annual risk assessment and all interim reviews.

Cyber Liability Insurance

VigiLife holds cyber liability insurance with sufficient coverage based on the organization's risk profile.

Our current cyber policy is covered by .

Fraud Risks

Due to its transparent culture, team size and operating model, including separation of duties, comprehensive controls, continuous monitoring and auditing, VigiLife considers its fraud-related risk to be very low.

VigiLife hires to perform accounting services and annual financial audits.

Fraud risk is re-evaluated as part of the organization's annual risk assessment. The assessment considers the following aspects of fraud:

- Pressures and/or incentives
- Opportunities
- Rationalities

Financial-related fraud assessment is led by the COO/CFO.

IT-related fraud assessment is led by the Compliance Officer or CISO.

Potential Frauds and Likelihood

Fraud Risk	Likelihood	In Place Controls/Monitors
Fraudulent Financial Reporting	Low	Monthly executive team reviews of business plan and revenue; Financial review by external accounting firm
Misappropriation of Assets	Low	Expense reporting and asset tracking in place
Regulatory and Legal Misconduct	Low	Audit and compliance policies and processes, including whistleblower procedures; engage external law firm to review legal conduct
Payroll Fraud	Low	Payroll is reviewed by at least two people internally as well as by external accounting firm
Kickbacks / Conflict of Interest	Low	Team-based vendor review and selection process
Misuse of Cloud Resources	Low	Continuous resource monitoring for all cloud accounts and regions and expense monitoring
Other IT Fraud	Low	IT assets and resources tracking

Compliance Audits and External Communications

2024.05.09

VigiLife may be requested occasionally to share additional details regarding its compliance, privacy and security program by an external entity such as a customer, media, legal or law enforcement. Such external communication, beyond what is already publicly published, needs to comply with the following policies and procedures.

Policy Statements

VigiLife policy requires that:

(a) VigiLife operations must comply with all applicable laws, regulations, security standards and frameworks. External audits shall be conducted accordingly to each applicable compliance requirement.

- HIPAA. VigiLife must comply with all requirements listed in the HIPAA (Health Insurance Portability and Accountability Act of 1996)

(b) All external communications related to compliance and customer/employee privacy must follow pre-established procedures and handled by approved personnel. This includes but is not limited to distribution of audit reports, assessment results, incidents and breach notification.

(c) Audit and compliance reports may be shared with an external party only when under signed NDA and approved by VigiLife Security and/or Privacy Officer.

Controls & Procedures

Compliance Program Management

VigiLife management and security/compliance team has identified and regularly reviews all relevant statutory, regulatory, and contractual requirements.

VigiLife's compliance policy includes requirements to meet any and all applicable compliance requirements.

Additionally, the Vendor Risk Management policies and procedures specify the details related to contractual agreements with clients, partners and vendors, as well as requirements and process related to intellectual property rights and the use of proprietary software products.

Requesting Audit and Compliance Reports

VigiLife, at its sole discretion, shares audit reports, including any Corrective Action Plans (CAPs) and exceptions, with customers on a case by case basis. All audit reports are shared under explicit NDA in VigiLife format between VigiLife and party to receive materials. Audit reports can be requested by VigiLife workforce members for Customers or directly by VigiLife Customers.

The following process is used to request audit reports:

1. A request may be sent by email to compliance@vigilife.com or by submitting a request via VigiLife Internal Support Portal or Email. In the request, please specify the type of report being requested and any required timelines for the report.
2. An Issue with the details of the request into the VigiLife Security Project on GitHub Issues, which is used to track requests status and outcomes.
3. VigiLife security team will confirm if a current NDA is in place with the party requesting the audit report. If there is no NDA in place, VigiLife will send one for execution.
4. Once it has been confirmed that an NDA is executed, VigiLife staff will move the GitHub Issues Issue to "Under Review".
5. The VigiLife Security Officer or Privacy Officer must Approve or Reject the Issue. If the Issue is rejected, VigiLife will notify the requesting party that we cannot share the requested report.
6. If the Issue has been Approved, VigiLife will send the customer the requested audit report and complete the GitHub Issues Issue for the request.

See detailed policy and procedures in Breach Notification

External Audits of Information Access and Activity

Prior to contracting with an external audit firm, VigiLife shall:

- Outline the audit responsibility, authority, and accountability
- Choose an audit firm that is independent of other organizational operations
- Ensure technical competence of the audit firm staff
- Require the audit firm's adherence to applicable codes of professional ethics
- Assign organizational responsibility for supervision of the external audit firm
- Obtain a signed HIPAA business associate agreement, if any ePHI will be shared/accessed during the audit

Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services to ensure separation of duties).

Contacts for External Communications Requests

Direct all other communication requests to one of the following:

- For incident reporting, vulnerability disclosure and other security related inquiries:

    - security@vigilife.com
    - https://www.vigilife.com/security
- For privacy concerns, including report of violation:
    - privacy@vigilife.com
    - https://www.vigilife.com/privacy
- For all compliance related issues, including request of audit reports:
    - compliance@vigilife.com

Continuous Compliance Monitoring

The status of compliance is tracked via . Compliance dashboards are configured with applicable internal and external standards and frameworks. Any potential gaps detected are reported on the compliance dashboards.

System Audits, Monitoring and Assessments

2024.02.13

VigiLife shall audit, monitor, and assess the access and activity of systems and applications that process or store production and/or sensitive data such as personally identifiable information (PII) and electronic protected health information (ePHI) in order to ensure compliance.

It is required by the HIPAA Security Rule, that healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Audit activities may be limited by application, system, and/or network auditing capabilities and resources. VigiLife shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

It is the policy of VigiLife to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, VigiLife shall audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions;
- Breaches in confidentiality and security of sensitive information;
- Performance problems and flaws in applications;
- Improper alteration or destruction of sensitive information;
- Out of date software and/or software known to have vulnerabilities.

This policy applies to all VigiLife systems that store, transmit, or process sensitive information.

Policy Statements

VigiLife policy requires that:

(a) All critical computing systems and software, both virtual and physical, must enable audit logging.

(b) Audit logs must include sufficient information to identify who did what, when, where.

(c) An annual audit of VigiLife security controls must be conducted, either by a designated internal audit team or a qualified external audit firm.

Controls & Procedures

Types of System Audits

VigiLife's auditing processes include the following.

1. **Configuration and Activity Monitoring:** This refers to the logging, monitoring, scanning and alerting of a system, account, or environment, which may be achieved using real-time automated scripts/software or a manual review/testing. This type of auditing is performed *continuously* as part of VigiLife operations.

Examples include:

* User: User and account-level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
* Application: Application-level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
* System: System-level audit trails generally monitor and log user activities, applications accessed, file integrity, and other system-defined specific actions.

* Network: Network-level scans or audit trails generally monitor information on what is operating, perform penetrations, and identify vulnerabilities.
* Traffic: Traffic refers to the incoming and outgoing traffic into and out of production/restricted environments. For example, firewall logs or VPC flow logs in AWS.
* Data: Data includes all successful and failed attempts at production data access and editing.

Data associated with above events will include origin, destination, action performed, timestamp, and other relevant details available.

2. **Access Review:** This refers to the review of all user and service accounts and permissions across VigiLife operational environments, including on-premise systems, cloud environments such as AWS accounts, and other applications such as collaboration software, ticketing system and code repos.

* VigiLife developed an internal tool to automatically pull configurations from our cloud based environments, including
  - AWS access configuration from IAM policies, EC2 VPC and security group settings, S3 bucket policies, Lambda and API Gateway resources, etc.;
  - Users, groups, application access from Okta IdP;
  - Network access settings from Cisco Meraki, etc.
* The data is collected either on demand triggered by security team or by changes in the operational environment.
* The data is used by the tool to aggregate and analyze user and application access.
* Access to other systems and applications that are not covered by this automated tool are reviewed manually on a quarterly basis or with any significant change to the target environment.
* As a result of each review, unused or invalid access will be removed.

3. **Compliance and Controls Audit:** This refers to the audit performed against the Technical, Administrative, and/or Physical controls as defined in VigiLife policies and procedures, to measure their adoption and effectiveness. This type of auditing is typically performed by either a designated internal audit team or an external audit firm, at *defined intervals* or prompted by a *trigger event*.

Potential trigger events include:

* Scheduled compliance audit/assessment (e.g. annual risk assessment)
* High risk or problem prone incidents or events, or as part of post-incident activities
* Business associate, customer, or partner complaints
* Identification of significant security vulnerabilities
* Atypical patterns of activity
* Failed authentication attempts
* Remote access use and activity
* Activity post termination
* Random audits

Security Events Analysis

Security logs, events, and audit trails are reviewed by the security team with the assistance of automated systems and processes.

- Auditing logs are automatically analyzed and correlated by the monitoring solutions and/or a centralized security information and event management system.
- The systems are configured with rules/policies to identify suspicious activities, vulnerabilities and misconfigurations.
- Alerts are triggered upon identification of an issue based on the policy configuration.
- The alerts are sent immediately to the responsible staff (e.g. security team) for analysis. The alerts may be sent via email, Slack messaging, or as notification on the monitoring dashboard.
- Analysis is prioritized based on alert severity. High severity alerts are typically reviewed within 24 hours.
- Incident response process is followed, as needed.
- Patches and updates will be applied to all systems in a timely manner.

Internal/Manual Auditing Activities

Additional manual reviews, such as user accounts and access auditing, may be necessary from time to time. These activities may be triggered by the events listed above.

- Responsibility for audit activity is assigned to VigiLife's Security Officer. The Security Officer shall:
    - Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
    - Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
    - Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).
    - All connections to VigiLife are monitored. Access is limited to certain services, ports, and destinations. Exceptions to these rules, if created, are reviewed on an annual basis.
- The manual review process shall define and include:
    - Description of the activity as well as rationale for performing the audit.
    - Identification of personnel to perform the review (workforce members shall not review audit logs that pertain to their own

system activity).
    - Frequency of the auditing process.
    - Determination of significant events requiring further review and follow-up.
    - Identification of appropriate reporting channels for audit results and required follow-up.
- Manual audits and reviews activities are tracked in GitHub Issues.
- Auditing, reviews and testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services to ensure separation of duties).

Audit Requests

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, Security Officer, Customer, Partner, or an Application owner or application user.
2. A request for an audit for specific cause must include time frame, frequency, and nature of the request.
3. A request for an audit must be reviewed and approved by VigiLife's Privacy Officer and/or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.
    - Should the audit disclose that a workforce member has accessed sensitive data inappropriately, the minimum necessary/least privileged information shall be shared with VigiLife's Security Officer to determine appropriate sanction/corrective disciplinary action.
    - Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by VigiLife's Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that VigiLife consider seeking guidance from risk management and/or legal counsel.

Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner, at least monthly, by the responsible workforce member(s). Additional reviews are performed as needed to assure the proper data is being captured and retained.
2. The reporting process shall allow for meaningful communication of the audit findings to relevant workforce members, Customers, or Partners.
    - Significant findings shall be reported immediately in a written format. VigiLife's security incident response form may be utilized to report a single event.
    - Routine findings shall be reported to the sponsoring leadership structure in a written report format.
3. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
4. Security audits constitute an internal, confidential monitoring practice that may be included in VigiLife's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative-level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable information shall not be included in the reports).
5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.

Remediation of Control Deficiencies

Most controls are continuously monitored and reported via automation on the platform.

Control deficiencies identified as a result of an internal or external system audit are documented and reviewed with management.

Security team works with the corresponding control owner to prioritize and mitigate the control deficiency, including applying corrective actions, implementating additional controls or adjusting existing controls as needed.

Audit Trails and Application Security Events Logging Standard

VigiLife logging standards requires application and system logs to contain sufficient information to determine **who did what, when, where** to ensure recording of security and audit events and to generate evidence for unauthorized activities.

All systems and software developed at VigiLife must have the following security events logging enabled as part of or in addition to standard application logging.

1. All security log events must have the following attributes at minimum:

1. All security log events must have the following attributes at minimum:
    - Timestamp of the event (synchronized to approved time server)
    - Identifier of the principal performing the action (such as user ID)
    - Location including both origin (such as hostname/IP) and target (such as host/service/resource)
    - Activity or action (such as log in, log out, create, read, update, delete of a resource)
        - the action may be logged as and determined by the HTTP request method and the API endpoint
    - Event description and additional details may be logged depending on the system or application
2. The following types of security events must be logged at minimum:
    - User and group administration activities (user or group added, updated, deleted, access granted/revoked)
    - All login attempts, successful and unsuccessful including the source IP address
    - All interactive logoffs
    - Privileged actions (configuration changes, application shutdown/restart, software update etc)
    - Major application events (e.g. application failure, start and restart, shutdown)
    - Any and all actions performed on critical resources such as production data
3. All application and system logs must not include (removed or masked):
    - Any sensitive information, including protected health information (PHI), personally identifiable information (PII)
        - except for IP addresses
        - usernames/logins may/should be logged as part of authentication logging
        - for user action auditing, opaque IDs should be used instead of usernames/logins whenever possible
    - Authentication and session tokens, user credentials
4. Security events and audit logs must be:
    - Always accessible to the monitoring system/team
    - Protected from any changes
    - Monitored with alerting mechanism in place (including alert for not receiving log events for a certain period of time)
5. All VigiLife IT infrastructure must have system clock synchronized

Examples of recommended application events for logging and their auditing purpose:

Events	Purpose
Client requests and server responses	forensics and debugging - details level is defined by application
Successful and unsuccessful login attempts	authentication
Successful and failed access to application resources	authorization, escalation of privileges
Excessive amount of requests from the client	brute-forcing, malicious bots, denial of service attacks
E-mails sent by an application	spamming, social engineering

Details of the logging configuration is documented at

- Application Logging - documented on the Engineering Wiki
- Identity and Access Activity Logs via Okta
- AWS Cloudtrail
- AWS S3 Server Access Logs

Audit Trail Integrity - Security Controls and Log Retention

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.
3. Whenever possible, audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges.
    - Separate systems are used to apply the security principle of "separation of duties" to protect audit trails from hackers.
    - VigiLife logging servers may include Elasticsearch, Logstash, and Kibana (ELK) as part of their baseline configuration to ease reviewing of audit log data. The ELK toolkit provides message summarization, reduction, and reporting functionality.
4. Reports summarizing audit activities shall be retained for a period of seven years.
5. Audit log data is retained locally on the audit log server or in the source environment for a period of one month. Beyond that, log data is encrypted and moved to warm storage (currently S3) using automated scripts, and is retained for a minimum of one year.

6. Raw event data may be purged after one month / 30 days as long as the required details are sufficiently covered in aggregated audit logs/reports.

Auditing Customer and Partner Activity

1. Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between VigiLife and the 3rd party. VigiLife will make every effort to assure Customers and Partners do not gain access to data outside of their own environments.
2. If it is determined that the Customer or Partner has exceeded the scope of access privileges, VigiLife's management and security must remedy the problem immediately.
3. If it is determined that a Customer or Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, VigiLife must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

Auditing and Assessment Tools

VigiLife's Security Officer is authorized to select and use assessment tools that are designed to detect vulnerabilities and intrusions. Use of such tools against VigiLife systems and environments are prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

- Scanning tools and devices;
- Password cracking utilities;
- Network "sniffers";
- Security agents installed locally on servers and endpoints;
- Passive and active intrusion detection systems; and
- Penetration testing tools.

Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

Training, Education, Awareness and Responsibilities

1. VigiLife workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and data. VigiLife's commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. VigiLife workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.
2. VigiLife Customers are provided with necessary information to understand VigiLife auditing capabilities. Platform Customers are responsible for the logging, auditing and retention of any application hosted outside of VigiLife environments, even though the applications may integrate with VigiLife Platform API. Customer applications hosted within the VigiLife environments will follow the auditing standards and procedures defined in this document.

HR and Personnel Security

2024.04.17

VigiLife is committed to ensuring all workforce members actively address security and compliance in their roles at VigiLife. We encourage self management and reward the right behaviors. This policy specifies acceptable use of end-user computing devices and technology. Additionally, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

Policy Statements

In addition to the roles and responsibilities stated earlier, VigiLife policy requires all workforce members to comply with the Acceptable Use Policy for End-use Computing and HR Security Policy.

VigiLife policy requires that:

(a) Background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the

perceived risk.

(b) Employees and independent contractors must agree and sign the terms and conditions of their offer letter or employment contract, and comply with acceptable use.

(c) Employees will go through an onboarding process that familiarizes them with the environments, systems, security requirements, and procedures VigiLife has in place. Employees will also have ongoing security awareness training that is audited.

(d) Employee offboarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any VigiLife systems has been removed, as well as ensuring that all company owned assets are returned.

(e) VigiLife and its employees will take reasonable measures to ensure no sensitive data is transmitted via digital communications such as email or posted on social media outlets.

(f) VigiLife will maintain a list of principles and values that will be part of onboarding procedures and have training available if/when the list of those activities changes. Examples of prohibited activities will also be provided for reference.

(g) A fair disciplinary process will be utilized for employees that are suspected of committing breaches of security. Multiple factors will be considered when deciding the response such as whether or not this was a first offense, training, business contracts, etc. VigiLife reserves the right to terminate employees in the case of serious cases of misconduct.

Controls & Procedures

HR Management and Reporting

VigiLife uses to manage its workforce personnel records.

Organization Structure

A reporting structure has been established that aligns with the organization's business lines and/or individual's functional roles. The organizational chart is available to all employees via .

Job Functions and Descriptions

Position / Job descriptions are documented and updated as needed that define the skills, responsibilities, and knowledge levels required for certain jobs.

Performance Reviews and Feedback

Employees receive regular feedback and acknowledgement from their manager and peers. Formal performance reviews are conducted annually using the company approved template, and stored on . Performance measures, incentives, and other rewards are established by management according to responsibilities at all levels, reflecting appropriate dimensions of performance and expected standards of conduct.

Acceptable Use of End-user Computing

VigiLife requires all workforce members to comply with the following acceptable use requirements and procedures, such that:

(a) Per VigiLife security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of VigiLife computing systems is subject to monitoring by VigiLife IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license installed through a pre-approved application store. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that may be affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the VigiLife Data Classification specifications and Data Handling

(i) All data storage devices and media must be managed according to the VigiLife Data Classification specifications and Data Handling procedures.

(j) It is strictly forbidden to download or store any sensitive data on end-user computing devices, including laptops, workstations and mobile devices.

(k) Mobile devices are not allowed to connect directly to VigiLife production environments.

Employee Screening Procedures

VigiLife publishes job descriptions for available positions and conducts interviews to assess a candidates technical skills as well as culture fit prior to hiring.

Background checks of an employee or contractor is performed by HR/operations and/or the hiring team prior to the start date of employment.

Employee Onboarding Procedures

A master checklist for employee onboarding is maintained by HR/Facilities and stored in Github.

The HR Representative / Facility Manager is responsible to create an Issue in the GitHub Issues HR & Facilities project to initiate and track the onboarding process. The onboarding process should include the following IT/Security items:

1. Training.
    - New workforce member is provided training on VigiLife security policy, acceptable use policy, and given access to the Employee Handbook.
    - HIPAA awareness training is provided to new workforce member.
    - Records of training and policy acceptance is kept in .
    - The training and acceptance must be completed within 30 days of employment.
2. Access.
    - Standard access is provisioned according to the job role and approval as specified in the HR onboarding GitHub Issues ticket.
    - Non-standard access requires additional approval following the access request procedures.
    - Request for modifications of access for any VigiLife employee can be made using the procedures outlined in the Access Establishment and Modification policy and procedures.
3. System configuration.
    - The end-user computing device (e.g. workstation or laptop) may be provisioned by IT to install necessary software, malware protection, security agents, and setting system configurations.
    - Users in a technical role, such as Development, may choose to self configure their system. In this case, the user is given configuration guidelines defined by IT and Security. The system must have the required security configuration and endpoint agents installed for monitoring and to ensure compliance.

Employee Exiting/Termination Procedures

A master checklist for employee existing/termination is maintained in .

1. The Human Resources Department (or other designated department), users, and their supervisors (HR) are required to notify the Security Team upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. HR are required to notify Security to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
    - The user has been using their access rights inappropriately;
    - A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
    - An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
3. A representative from the Security Team will terminate users' access rights immediately upon notification, and will coordinate with the appropriate VigiLife employees to terminate access to any non-production systems managed by those employees.
4. Security audits and may terminate access of users that have not logged into organization's information systems/applications for an extended period of time.

Employee Issue Escalation

VigiLife workforce members are to escalate issues using the procedures outlined in the Employee Quick Reference. Issues that are brought to the Escalation Team are assigned an owner. The membership of the Escalation Team is maintained by the Chief Executive Officer or his delegate.

Security incidents, particularly those involving sensitive data, are handled using the process described in Incident Response. If the incident involves a breach of sensitive data, the Security Officer will manage the incident using the process described in Breach Notification. Refer to Incident Response for a list of sample items that can trigger VigiLife's incident response procedures; if you are unsure whether the issue is a security incident, contact the Security team immediately.

It is the duty of the incident owner to follow the process outlined below:

1. Create an Issue in the GitHub Issues Security Project.
2. The Issue is investigated, documented, and, when a conclusion or remediation is reached, it is moved to Review.
3. The Issue is reviewed by another member of the Security or HR team. If the Issue is rejected, it goes back for further evaluation and review.
4. If the Issue is approved, it is marked as Done, adding any pertinent notes required.
5. The workforce member that initiated the process is notified of the outcome via email.

Whistleblower Policy and Process

The VigiLife requires all workforce members to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. All workforce members must practice honesty and integrity in fulfilling their responsibilities and comply with all applicable laws and regulations.

(a) Reporting Responsibility. Each workforce member is required and encouraged to report serious concerns so that VigiLife can address and correct inappropriate internal conduct and actions. This includes

- questionable or improper accounting or auditing matters,
- violations and suspected violations of company policies or ethics, or
- suspected violations of law or regulations that govern VigiLife’s operations

(b) Acting in Good Faith. Anyone filing a written complaint concerning a violation or suspected violation must be acting in good faith and have reasonable grounds for believing the information disclosed indicates a violation. Any allegations that prove not to be substantiated and which prove to have been made maliciously or knowingly to be false will be viewed as a serious disciplinary offense.

(c) Confidentiality. Insofar as possible, the confidentiality of the whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law, and to provide accused individuals their legal rights of defense.

(d) No Retaliation. Workforce members, in good faith, reporting a concern under the Whistleblower Policy shall NOT be subject to retaliation or adverse employment consequences. Moreover, any workforce member who retaliates against someone who has reported a concern in good faith is subject to disciplinary actions up to and including termination of employment.

(e) Reporting. Reports of concerns may be filed directly with the company CEO. Additional reporting procedure details can be found in the employee handbook.

Employee Performance Review Process

Formal performance reviews are conducted annually using .

- Employee provides their own self assessment for both performance outcome and behavior
- Manager reviews employee self-assessment and peer feedback, and documents the final review and rating
- The final review and rating is reviewed and signed by both the employee and their manager

Employee Incentives and Rewards

VigiLife encourages employees to go above and beyond to contribute to the business objectives and help their peers and customers. Employees are recognized and rewarded for positive behavior on a regular basis via peer recognition, appreciation, and feedback.

Continuous Education and Skills Development

VigiLife provides employees the opportunity to attend conferences, trade shows, and/or ongoing training/studies relevant to their job function and business objectives.

Non-Compliance Investigation and Sanctions

Workforce members shall report non-compliance of VigiLife's policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

1. The Security Officer promptly facilitates a thorough investigation of all reported violations of VigiLife's security policies and procedures. The Security Officer may request the assistance from others.
    - Complete an audit trail/log to identify and verify the violation and sequence of events.
    - Interview any individual that may be aware of or involved in the incident.
    - All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
    - Provide individuals suspected of non-compliance of the Security rule and/or VigiLife's policies and procedures the opportunity to explain their actions.
    - The investigator thoroughly documents the investigation as the investigation occurs. This documentation must include a list of all employees involved in the violation.
2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
    - A fair disciplinary process will be utilized for employees are suspected of committing breaches of security. Multiple factors will be considered when deciding the response such as whether or not this was a first offense, training, business contracts, etc.
    - VigiLife reserves the right to terminate employees in the case of serious cases of misconduct.
    - A violation resulting in a breach of confidentiality (i.e. release of sensitive data to an unauthorized individual), change of the data integrity, or inability to access data by other users, requires immediate termination of the workforce member from VigiLife.
3. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
4. In the case of an insider threat, the Security Officer and Privacy Officer are to set up a team to investigate and mitigate the risk of insider malicious activity. VigiLife workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.
5. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of seven years after the conclusion of the investigation.
6. When the Security Officer identifies a violation and begins a formal sanction process, they will notify the appropriate management or supervisors within 24 hours. That notification will include 1) identifying the individual sanctioned, 2) the reason for the sanction, and 3) specific procedures for service or account restriction / revocation or other disciplinary actions as required.

    Warning Notice Template

Access

2024.02.13

Access to VigiLife systems and application is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems.

These safeguards have been established to address the HIPAA Security regulations and industry best practices.

Policy Statements
Access Control Policy

VigiLife policy requires that

(a) Access to all computing resources, including servers, end-user computing devices, network equipment, services and applications, must be protected by strong authentication, authorization, and auditing.

(b) Interactive user access must be associated to an account or login unique to each user.

(c) All credentials, including user passwords, service accounts, and access keys, must meet the length, complexity, age, and rotation requirements defined in VigiLife security standards.

(d) Use strong password and multi-factor authentication (MFA) whenever possible to authenticate to all computing resources (including both devices and applications).

(e) MFA is required to access any critical system or resource, including but not limited to resources in VigiLife production environments.

(f) Unused accounts, passwords, access keys must be removed within an established timeframe.

(g) A unique access key or service account must be used for different application or user access.

(h) Authenticated sessions must time out after a defined period of inactivity.

Access Authorization and Termination

VigiLife policy requires that

(a) Access authorization shall be implemented using role-based access control (RBAC) or similar mechanism.

(b) Standard access based on a user's job role may be pre-provisioned during employee onboarding. All subsequent access requests to computing resources must be approved by the requestor's manager, prior to granting and provisioning of access.

(c) Access to critical resources, such as production environments, must be approved by the security team in addition to the requestor's manager.

(d) Access must be reviewed on a regular basis and revoked if no longer needed.

(e) Upon termination of employment, all system access must be revoked and user accounts terminated within the defined, predetermined timeframe.

(f) All system access must be reviewed at least annually and whenever a user's job role changes.

Shared Secrets Management

VigiLife policy requires that

(a) Use of shared credentials/secrets must be minimized and approved on an exception basis.

(b) If required by business operations, secrets/credentials must be shared securely and stored in encrypted vaults that meet the VigiLife data encryption standards.

(c) Usage of a shared secret to access a critical system or resource must be supported by a complimenting solution to uniquely identify the user.

Privileged Access Management

VigiLife policy requires that

(a) Users must not log in directly to systems as a privileged user.

- A privileged user is someone who has administrative access to critical systems, such as a Active Directory Domain Administrator, root user to a Linux/Unix system, and Administrator or Root User to an AWS account.

(b) Privilege access must only be gained through a proxy, or equivalent, that supports strong authentication (such as MFA) using a unique individual account with full auditing of user activities.

(c) Direct administrative access to production systems must be kept to an absolute minimum.

Controls & Procedures

Standards for Access Provisioning
Workforce Clearance

1. The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are treated on a "least-privilege" principle.
3. VigiLife maintains a minimum necessary approach to access to Customer data. As such, VigiLife, including all workforce members, does not readily have access to any ePHI.

Access Authorization

1. Role based access categories for each VigiLife system and application are pre-approved by the Security Officer.

2. VigiLife utilizes hardware-defined and/or software-defined boundaries to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.

Person or Entity Authentication

1. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
2. Each cloud user has and uses a unique user ID and password or OpenID Connect that identifies him/her as the user of the information system. This is enforced through the use of **AWS Identity Center**.
3. All customer support interactions must be verified before VigiLife support personnel will satisfy any request having information security implications.

Unique User Identification

1. Access to the VigiLife Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
2. Passwords requirements mandate strong password controls (see below).
3. Passwords are not displayed at any time and are not transmitted or stored in plain text.
4. Default accounts on all production systems and environments, including root, are disabled/locked.
5. Shared accounts are not allowed within VigiLife systems or networks.

Automatic Logon and Logoff

1. Automated log-on configurations that store user passwords or bypass password entry are not permitted for use with VigiLife workstations or production systems.
    - Automatic log-on may only be permitted for low-risk systems such as conference room PCs connecting to a Zoom Room.
    - Such systems are configured on separate network VLANs.
2. Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
3. Information systems automatically lock users such as enabling password-protected screensaver after 2 minutes or less of inactivity.
4. Information systems automatically enter standby or log users off the systems after 30 minutes or less of inactivity.
5. The Security Officer must pre-approves any exception to automatic log off requirements.

Password Management

1. User IDs and passwords are used to control access to VigiLife systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the VigiLife environment, password configurations are set to require:
    - a minimum length of 8 characters;
    - a mix of upper case characters, lower case characters, and numbers or special characters;
    - a annual password expiration
    - prevention of password reuse
    - where supported, modifying at least 6 characters when changing passwords;
    - where supported, temporary account lockout after 5 invalid attempts.

Exceptions

Password expiration may be set to a greater interval if an account is always protected by MFA.

4. All system and application passwords must be stored and transmitted securely.

* Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or stronger NIST compliant standard).
* Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in [Data Protection](/data-protection/).
* Transmitted passwords must be encrypted in flight pursuant to the requirements in [Data Protection](/data-protection/).

5. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the system owner and/or Security, based on the criticality and sensitivity of the data contained within the network, system, application, and/or database.

1. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in HR policy).
2. All default system, application, and Vendor/Partner-provided passwords are changed before deployment to production.
3. Upon initial login, users must change any passwords that were automatically generated for them.
4. Password change methods must use a confirmation method to correct for user input errors.
5. All passwords used in configuration scripts are secured and encrypted.

6. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security team.
7. In cases where a user has forgotten their password, password reset procedures provided by the IdP shall be followed. The exact

7. In cases where a user has forgotten their password, password reset procedures provided by the IdP shall be followed. The exact process depends on the system or application. If help is needed, users shall contact IT Support or Security
8. An approved password manager is used for to store or share non-critical business application passwords that are not integrated with our primary IdP through SSO.
    - The password manager locally encrypts the password vault with the user's master password before synchronizing to the cloud.
    - The master password must follow the password requirements listed above.
    - MFA must enabled in the password manager configuration.
    - Enrollment of the password manager is configured as an application in Keeper.
9. An automated process/tool is implemented to ensure compromised passwords or common dictionary words are not used as passwords. This is currently implemented in Keeper.

Single Sign On

- VigiLife selected Azure Active Directory as its primary Identity Provider (IdP) to control user access to systems and business applications.
- Single sign-on (SSO) should be used whenever possible instead of local authentication. This centralized approach improves user experience and simplifies access management.
- SSO is configured via industry standard SAML protocol between the IdP (Azure Active Directory) and the target application.
- VigiLife will not configure SSO to target applications unless they score a "B" rating or higher on the Qualys SSL Labs benchmark.
- Security team is responsible for the administration of the IdP / SSO system, including user and access provisioning. Security team may delegate administrative privilege to a subset of the system, such as a specific application.

Multi-factor Authentication

Multi-factor authentication (MFA) is a standard control used by VigiLife to provide strong access control to critical systems and applications, and should be enabled whenever possible.

VigiLife uses Azure Active Directory for MFA.

Important

Approved MFA methods include:

- Push notification delivered through the MFA provider's mobile app (default and preferred for end-user access)
- Hardware MFA token (required for the root user of AWS accounts)
- A unique cryptographic certificate tied to a device
- Time-based One-Time Password (TOTP) delivered through a mobile app, such as Google Authenticator
- One-time passcode delivered through SMS text message (if it is the only supported option)
- Secure physical facility (if the system or application can only be accessed at that location)

Role Based Access Control (RBAC)

By default, user access is granted based on the user's job function / role. For example:

- Developer
- Security
- IT
- Administrative
- Marketing / Sales

This is defined as **user groups** in .

Access to sensitive data and production customer data is highly restricted and further defined in its own section.

Access to AWS Accounts and Resources

Access to VigiLife AWS accounts are permissible through AWS Identity Services.

Identity services is a resilient and highly available way to manage identities, permissions, and resource access. VigiLife can grant employees the access they need using fine-grained permissions, organizational and account governance, as well as preventative, detective, and proactive security controls.

AWS Organizations

In addition to AWS Identity services VigiLife also uses AWS Organizations

AWS Organizations offers the following features:

- Centralized management of all AWS accounts
- Hierarchical grouping of AWS accounts to meet budgetary, security, and compliance needs
- Policies to centralize control over the AWS services and API actions that each account can access.
- Policies to standardize tags across the resources in VigiLife accounts
- Policies that configure automatic backups for the resources in your organization's accounts
- Integration and support for AWS Identity and Access Management (IAM)

Access to PHI/ePHI

1. Access to ePHI is permitted to insights/analytics staff, or staff that otherwise has a business need to access.
2. Access to ePHI in VigiLife's production environments in the cloud is strictly prohibited. Access is protected via multiple layers of security controls such as IAM policies, restricted IAM roles, VPC configuration, S3 bucket policy, external monitoring, etc.
3. Users may not download non-anonymoized ePHI to any workstations or end-user computing devices.

Platform Customer Access to Systems

VigiLife does not allow direct system access by customers. Access is only available through the Web UI or mobile app, with valid authentication and authorization.

Access Establishment, Modification and Termination

1. Requests for access to VigiLife Platform systems and applications is made formally using the following process:
    1. An access request is created in GitHub Issues through either the new employee onboarding request
    2. The Security team will grant standard access to per job role as part of new employee onboarding. A standard set of accounts that are default for all employees are created as part of the onboarding process. This includes
        - User account for local system/laptop
        - Office365 account for access to Outlook email, SharePoint, etc.
        - KnowB4 account for security awareness training
        - HR accounts for paperwork, benefits management, payroll, expense reporting, etc.
        - Additional role based access (e.g. GitHub and GitHub Actions access for a developer)
    3. Standard access may be provisioned at any time by account owners/administrators at any time during or after onboarding with approval of account owners and/or manager.
    4. If additional access is needed in addition to the above, a separate access request (through GitHub Issues) is required and the requester must include a description and justification as part of the access request.
    5. Once the review is completed, the Security team approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
    6. If the review is approved, IT or Security team provisions access, then marks the Issue as Done, adding any pertinent notes required.
        - New accounts will be created with a temporary secure password that meets all password requirements, which must be changed on the initial login.
        - All password exchanges must occur over an authenticated channel.
        - For on-premise systems, access grants are accomplished by adding the appropriate user account to the corresponding LDAP/AD group.
        - For cloud accounts, access grants are provisioned using the access control mechanisms built in IAM and AWS Identity Center.
        - Account management for non-production systems may be delegated to a VigiLife employee at the discretion of the Security Officer.
2. Special access, including access to production environments, is not granted until receipt, review, and approval by the VigiLife Security Officer.
3. The request for access is retained for future reference.
4. Temporary accounts are not used unless absolutely necessary for business purposes.
    - Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily

- Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
    - Accounts that are inactive for over 90 days are removed.

5. In the case of non-personal information, such as generic educational content, identification and authentication may not be required.

Access Termination

IT Manager or Security team receives access termination requests in one of the following conditions and processes it accordingly:

- Employee existing/termination, as defined by the process in HR & Employee Security;
- Employee access to a system is no longer required as a result of job role change or similar event, in which case a access termination request may be submitted by the employee or his/her manager via the Internal Help portal or an email request to Security team;
- As the result of a Access Review, as defined in System Auditing.
- Non-standard access is revoked by default after 30 days of inactivity, unless an exception/extension is requested and approved.

Access Reviews

- All access to VigiLife systems and services are reviewed and updated following the procedures specified in System Auditing to ensure proper authorizations are in place commensurate with job functions.
- In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security and Privacy Officer to limit access and reduce risk of unauthorized access.

Privileged Access

Privileged users must first access systems using standard, unique user accounts before elevating the privilege or switching to privileged users and performing privileged tasks. Examples include:

- `sudo` in Linux/macOS
- `Run as Administrator` in Windows
- `Assume role` in AWS

Service Accounts

- All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
- Services that are part of VigiLife platform leverage AWS IAM policy configurations and/or OAuth for authorization.
- Generic accounts are not allowed on VigiLife systems.
- Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.
- In AWS, service accounts are implemented in the form of IAM Roles, and their access defined by the corresponding IAM policies. The creation of these IAM roles and policies is implemented as code, which follows the secure development, review and production change approval process.

Employee Workstation / Endpoints Access and Usage

All workstations at VigiLife are company owned, using one the following approved hardware vendors and operating systems:

- Apple, HP, Dell, or Lenovo
- macOS, Windows 10+

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization's system.
3. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
4. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
5. Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
6. Workstation hard drives will be encrypted using native encryption by the manufacturer, FileVault, BitLocker or equivalent.
7. All workstations must have host firewalls enabled to prevent unauthorized access unless explicitly granted.
8. All workstations must have endpoint security software installed and actively running, if supported by the operating system.

Production Access and Secrets Management

VigiLife leverages a combination of GitHub Actions, AWS System Manager Parameter Store, and AWS Secure Secrets Manager to securely store production secrets. Secrets are always encrypted; access to secrets is always controlled and audited.

Production Data Access

The following requirements and controls are in place for accessing production data by internal personnel:

- There is no pre-provisioned, persisted "internal" access to production data stores. Access such as direct SSH to the production database servers and direct access to data objects in production S3 buckets are prohibited.
- Access to customer data is granted on a per-account basis.
- Access requests follow the same production access processes. Access must be approved by both the data owner and the security team.
- Access to production data is granted only through an approved platform with strong centralized access control, with MFA.
- Access is revoked when no longer needed.

Password Reset and other Helpdesk Requests

VigiLife employees have the ability to obtain self-service support directly from supported business applications, such as password reset via the SSO/IdP tool.

If needed, users may use our internal service desk or email request to obtain IT and Security support.

A ticket is opened in GitHub Issues for each support request and assigned to the appropriate personnel. The person assigned must verify the identity of the requester and ensure the ticket has appropriate approval before implementing or providing support. The verification step and confirmation of "User identity verified" should be included as a comment in the ticket by the support personnel. Additionally, if a password or security credential has been created or supplied, confirm user has received it via another channel like slack/email/phone/zoom and document receipt in the ticket.

Facility Access and Physical Security

2024.02.13

It is the goal of VigiLife to provide a safe and secure environment for all employees. Access to the VigiLife facilities is limited to authorized individuals only.

VigiLife works with Subcontractors (e.g. property management companies and facilities management) to assure restriction of physical access to systems used as part of the VigiLife Platform.

Physical Access to all of VigiLife facilities is limited to only those authorized in this policy. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to VigiLife's facility.

VigiLife and its Subcontractors control access to the physical buildings/facilities that house these systems/applications, or in which VigiLife workforce members operate, in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. In an effort to safeguard ePHI from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with escorts for unauthorized persons.

Policy Statements

VigiLife policy requires that

(a) Physical access to VigiLife facilities is restricted.

(b) All employees are required to wear employee badges at secure facilities (such as server rooms, data centers, labs).

(c) All employees must follow physical security requirements and procedures documented by facility management.

(d) On-site visitors and vendors must be escorted by a VigiLife employee at all times while on premise.

(e) All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to VigiLife's facility.

(f) Retain a record for each physical access, including visits, maintenance and repairs to VigiLife production environments and secure facilities.

- Details must be captured for all maintenance and repairs performed to physical security equipment such as locks, walls, doors, surveillance cameras; and
- All records must be retained for the defined, predetermined timeframe.

(g) Building security, such as fire extinguishers and detectors, escape routes, floor warden responsibilities, shall be maintained according to applicable laws and regulations.

Controls & Procedures

Physical Security
Access Requirements Overview

- Physical access is restricted using badge readers and/or smart locks that track all access.
    - Restricted areas and facilities are locked when unattended (where feasible).
    - Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
    - Access and keys are revoked upon termination of workforce members.
    - Workforce members must report a lost and/or stolen key(s) or badge(s) to his/her manager, local Site Lead, or the Facility Manager.
    - The Facility Manager or designee is responsible to revoke access to the lost/stolen badge(s) or access key(s), and re-provision access as needed.
    - The Facility Manager or designee facilitates the changing of the lock(s) within 7 days of a physical key being reported lost/stolen.
- Enforcement of Facility Access Policies
    - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
    - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
    - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from VigiLife.
- Workstation Security
    - Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
    - All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
    - All workstations purchased by VigiLife are the property of VigiLife and are distributed to users by the company.

Building Standards per Location

All entry points are secured by card readers and have cameras for additional monitoring as needed.

- **Dayton, OH** Office
    - The building is unlocked Monday-Friday from 7:30am-5pm
    - After hours the building is secured and requires a key for entry
    - VigiLife office space is secured and requires an access card for entry at all times
    - All server rooms are secured 24/7 and require an access card for entry
    - Physical security and monitoring to the building is managed by Aptima, Inc, who is the primary tenant of the office space

New Hires

New Hire access cards are assigned based on new hire notice issued through GitHub Issues.

- New Hire access is typically activated within 1 week of start date
- Once the access card is created it is stored in a locked cabinet until issued to new hire.

Separations

Separation notices are issued through GitHub Issues.

- Immediate separation notices are processed when issued
- Future separation notices are pre-scheduled for deactivation prior to termination date

Special Access Requests

Special access areas require additional approvals for access. If documented approver is unavailable, CEO may act as approver.

Maintenance & Repairs

All maintenance, repairs and modifications to our access control system will be handled by the local vendor that supports our system.

All documents regarding maintenance, repair or modification will be stored in the physical security folder located on the VigiLife SharePoint

site.

Reporting and Auditing

All access control records are audited on an annual basis.

Special access is audited and reviewed with approver quarterly.

Records are owned and maintained by the Facility Manager. Records are kept in the Physical Security folder on SharePoint and will be retained for a minimum of 3 years.

Data Center Security

Physical security of data centers is ensured by the cloud infrastructure service provided, .

Clean Desk Policy and Procedures

Employees must secure all sensitive/confidential information in their workspace at the conclusion of the work day and when away from their workspace. This includes both electronic and physical information such as:

- computer workstations, laptops, and tablets
- removable storage devices including CDs, DVDs, USB drives, and external hard drives
- printed materials

Computer workstations/laptops must be locked (password protected) when physically unattended. Portable devices such as laptops and tablets should be taken home at the conclusion of the work day.

Removable storage devices and printed documents must be treated as sensitive material and locked in a drawer or similar when not in use. Printed materials must be immediately removed from printers or fax machines. Passwords must not be written down or stored physically.

Keys and access cards used for access to sensitive or restricted information/areas must not be left unattended anywhere in the office.

Asset Inventory Management

2024.02.13

You can't protect what you can't see. Therefore, it is imperative for VigiLife to maintain an accurate and up-to-date inventory of both its physical and digital assets.

More details on data inventory and data lifecycle management is documented separately in Data Management.

Policy Statements

VigiLife policy requires that:

(a) IT and/or Security must maintain an inventory of all critical company assets, both physical and logical.

(b) All assets should have identified owners and be tagged with a risk/data classification.

(c) All physical assets must be labeled with a company property tag.

Controls & Procedures

Physical Asset Inventory

VigiLife IT leverages a SaaS-based IT asset management system, , to maintain inventory of all company owned physical computing equipment, including but not limited to:

- servers
- workstations
- laptops

- printers
- networking equipment

Each record includes details of the physical device such as manufacturer, model as well as ownership details and property tag ID.

The movement of computing hardware and electronic media is maintained as part of the records, including media re-use and ownership reassignment.

VigiLife IT manager is responsible for ensuring each physical asset is applied with a VigiLife property tag, and an up-to-date record is maintained in the IT asset management system.

All company-owned devices are subject to a complete data wipe if deemed necessary, such as in the case of device infection or repurpose. This data wipe will be carried out by the IT manager.

Digital Asset Inventory

VigiLife Security team uses an automated system to query across our cloud-based infrastructure, including but is not limited to AWS, to obtain detailed records of all digital assets, including but not limited to:

- Virtual machines
- AWS EC2 instances
- AWS S3 repositories
- AWS Lambda functions
- Security agents
- Source code repositories
- User accounts

The records are stored in a database system maintained by VigiLife security team. Records are tagged with owner/project and classification when applicable. All records are kept up to date via automation.

Paper Records

VigiLife does not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against VigiLife policies.

Data Management Policy

2024.04.17

This policy outlines the requirements and controls/procedures VigiLife has implemented to manage the end-to-end data lifecycle, from data creation/acquisition to retention and deletion.

Additionally, this policy outlines requirements and procedures to create and maintain retrievable exact copies of electronic protected health information(ePHI), PII and other critical customer/business data.

Data backup is an important part of the day-to-day operations of VigiLife. To protect the confidentiality, integrity, and availability of sensitive and critical data, both for VigiLife and VigiLife Customers, complete backups are done daily to assure that data remains available when it needed and in case of a disaster.

Policy Statements

VigiLife policy requires that

(a) Data should be classified at time of creation or acquisition according to the VigiLife data classification model, by labeling or tagging the data.

(b) Maintain an up-to-date inventory and data flows mapping of all critical data.

(c) All business data should be stored or replicated to a company controlled repository, including data on end-user computing systems.

(d) Data must be backed up according to its level defined in VigiLife data classification.

(e) Data backup must be validated for integrity.

(f) Data retention period must be defined and comply with any and all applicable regulatory and contractual requirements. More specifically,

- Data and records belonging to VigiLife platform customer must be retained per VigiLife product terms and conditions and/or specific contractual agreements.

(g) By default, all security documentation and audit trails are kept for a minimum of five years, unless otherwise specified by VigiLife data classification, specific regulations or contractual agreement.

Controls & Procedures

Data Classification Model

VigiLife defines the following four classifications of data:

- **Critical**
- **Confidential**
- **Internal**
- **Public**

Definitions and Examples

Critical data includes data that must be protected due to regulatory requirements, privacy, and/or security sensitivities.

Unauthorized disclosure of critical data may result in major disruption to business operations, significant cost, irreparable reputation damage, and/or legal prosecution to the company.

External disclosure of critical data is strictly prohibited without an approved process and agreement in place.

Example Critical Data Types includes

- PII
- PHI or ePHI
- Production Security data, such as
  - Production secrets, passwords, access keys, certificates, etc.
  - Production security audit logs, events, and incident data

Confidential and proprietary data represents company secrets and is of significant value to the company.

Unauthorized disclosure may result in disruption to business operations and loss in value.

Disclosure requires the signing of NDA and management approval.

Example Confidential Data Types includes

- Business plans
- Employee/HR data
- News and public announcements (pre-announcement)
- Patents (pre-filing)
- Specialized source codes
- Non-production Security data, including
  - Non-prod secrets, passwords, access keys, certificates, etc.
  - Non-prod security audit logs, events, reports, and incident data
  - Audit/compliance reports, security architecture docs, etc.

Internal data contains information used for internal operations.

Unauthorized disclosure may cause undesirable outcome to business operations.

Disclosure requires management approval. NDA is usually required but may be waived on a case-by-case basis.

Example Internal Data Types includes

- Internal documentation
- Policies and procedures
- Product roadmaps
- Most source codes

Public data is Information intended for public consumption. Although non-confidential, the integrity and availability of public data should be protected.

Example Internal Data Types includes

- News and public announcements (post-announcement)
- Marketing materials
- Product documentation
- Contents posted on company website(s) and social media channel(s)

Data Handling Requirements Matrix

Requirements for data handling, such as the need for encryption and the duration of retention, are defined according to the VigiLife Data Classifications.

Data	Labeling or Tagging	Segregated Storage	Endpoint Storage	Encrypt At Rest	Encrypt In Transit	Encrypt In Use	Controlled Access	Monitoring	Destruction at Disposal	Re
Critical	Required	Required	Prohibited	Required	Required	Required	Access is blocked to end users by default; Temporary access for privileged users only	Required	Required	
Confidential	Required	N/R	Allowed	Required	Required	Required	All access is based on need-to-know	Required	Required	
Internal	Required	N/R	Allowed	N/R	N/R	N/R	All employees and contractors (read); Data owners and authorized individuals (write)	N/R	N/R	
Public	N/R	N/R	Allowed	N/R	N/R	N/R	Everyone (read); Data owners and authorized individuals (write)	N/R	N/R	

N/R = Not Required

† Enterprise customer-owned data is stored for as long as their configured retention period, or as required by regulations.

Data Inventory and Lifecycle Management

VigiLife Security team uses an automated system to query across our cloud-based infrastructure, including but is not limited to AWS, to obtain detailed records of all data repositories, including but not limited to:

- AWS S3 repositories

- AWS RDS and DynamoDB instances
- AWS EC2 volumes
- Source code repositories
- Office 365
- On-premise storage systems (manually maintained)

The records are stored in a database system maintained by VigiLife security team. Records are tagged with owner/project and classification

when applicable. All records are kept up to date via automation. The system is also designed to track movement of data and update/alert accordingly.

AWS S3 Object Lifecycle Management

The VigiLife platform will automatically adjust the storage class for certain types of data based on its usage pattern and age. This allows the VigiLife platform to provide competitive pricing while still allowing the customer to store large amounts of data.

AWS provides the following storage classes as an example of this:

- General Purpose
- Infrequent Access
- Archive (Amazon Glacier)

VigiLife performs regular full backups of all production data using AWS Backup. We leverage lifecycle policies to automatically remove old backup data. This allows older data to "age out" instead of having to explicitly delete it.

Other Business Data

All internal and confidential business records and documents, such as product plans, business strategies, presentations and reports, are stored outside of an employee workstation or laptop.

- Official records are stored in record management systems such as
    - GitHub Issues (tickets),
    - GitHub (source code),
    - SharePoint
- Unstructured business documents such as Word documents, Excel spreadsheets and PowerPoint presentations are stored on VigiLife internal file share.
- Confidential business documents/records are be stored in encrypted form and with access control enabled on a need-to-know basis.

Transient Data Managemet

Data may be temporarily stored by a system for processing. For example, a storage device may be used to stage temp/raw files prior to being uploaded to the production environment in AWS. These transient data repositories are not intended for long term storage, and data is purged immediately after use.

VigiLife currently does NOT use transient storage for any sensitive data.

Backup and Recovery

Customer Data

VigiLife stores data in a secure production account in AWS, using a combination of services (e.g. S3, DynamoDB, TimeStream).

All data store services and platforms in use are HIPAA compliant.

VigiLife performs automatic backup of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process will back up all data to a separate AWS region in the same country (e.g. US East to US West). By default, data will be backed up at least daily. The backups are encrypted in the same way as live production data.

Source code

VigiLife stores its source in git repositories hosted by GitHub.

Source code repositories are backed up to VigiLife's AWS S3 infrastructure account on a weekly basis with a common set of configuration for each repository to enforce SDLC processes.

In the event that GitHub suffers a catastrophic loss of data, source code will be restored from the backups in AWS S3.

Business records and documents

Each data owner/creator is responsible for maintaining a backup copy of their business files local on their laptop/workstation to the appropriate location on VigiLife SharePoint team site. Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams

- Meeting notes/recordings
- Important records (e.g. approval notes)

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet VigiLife requirements).

Data Deletion Procedures

For patient data as as a Covered Entity

VigiLife is NOT a covered entity. Should we become a covered entity in the future, we would be required by law to retain healthcare records for up to 10 years beyond when service was last provided when providing healthcare services directly to patients. Any patient data that is marked for deletion will be archived for the time required by law. This archived data can be retrieved by the customer as long as it is retrieved within 10 years from date of last service.

Data Protection

2024.02.13

VigiLife takes the confidentiality and integrity of its customer data very seriously. As stewards and partners of VigiLife Customers, we strive

to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical controls in support of the VigiLife mission of data protection.

Production systems that create, receive, store, or transmit Customer data (hereafter "Production Systems") must follow the requirements and guidelines described in this section.

Policy Statements

VigiLife policy requires that:

(a) Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.

(b) Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorization, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.

(c) Workforce members shall not have direct administrative access to production data during normal business operations. Exceptions include emergency operations such as forensic analysis and manual disaster recovery.

(d) All Production Systems must disable services that are not required to achieve the business purpose or function of the system.

(e) All access to Production Systems must be logged, following the VigiLife Auditing Policy.

(f) All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.

Controls & Procedures

Data Protection Implementation and Processes

Data is classified and handled according to the VigiLife Data Handling Specifications and Data Classification document.

Critical, confidential and internal data will be tagged upon creation, if tagging is supported. Each tag maps to a data type defined in the data classification scheme, which then maps to a protection level for encryption, access control, backup, and retention. Data classification may alternatively be identified by its location/repository. For example, source codes in VigiLife's GitHub repos are considered "Internal" by default, even though a tag is not directly applied to each source file.

Critical and confidential data is always stored and transmitted securely, using approved encryption standards. More details are specified in VigiLife's Data Classification and Handling document.

All IT systems that process and store sensitive data follow the provisioning process, configuration, change management, patching and anti-malware standards as defined in Configuration and Change Management document.

Customer/Production Data Protection

VigiLife hosts on Amazon Web Services in the US-East (Ohio) region by default. Data is replicated across multiple regions for redundancy and disaster recovery.

All VigiLife employees, systems, and resources adhere to the following standards and processes to reduce the risk of compromise of Production Data:

1. Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
2. Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
3. Ensure VigiLife Customer Production Data is segmented and only accessible to Customer authorized to access data.
4. All Production Data at rest is stored on encrypted volumes using encryption keys managed by VigiLife. Encryption at rest is ensured through the use of automated deployment scripts referenced in Configuration and Change Management.
5. Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
6. Encrypted volumes use approved cipher algorithms, key strength, and key management process as defined in §12.3.1 above.
7. Raid volume drives are individually encrypted and assembled on boot requiring a manual input of the key to mount the encrypted volume.

Access

VigiLife employee access to production is guarded by an approval process and by default is disabled. When access is approved, temporary access is granted that allows access to production. Production access is reviewed by the security team on a case by case basis.

Separation

Customer data is logically separated at the database/datastore level using a unique identifier for the institution. The separation is enforced at the API layer where the client must authenticate with a chosen institution and then the customer unique identifier is included in the access token and used by the API to restrict access to data to the institution. All database/datastore queries then include the institution identifier.

Backup and Recovery

For details on the backup and recovery process, see controls and procedures defined in Data Management.

Monitoring

VigiLife uses AWS CloudWatch/CloudTrail to monitor the entire cloud service operation. If a system failure and alarm is triggered, key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action. Escalation may be required and there is an on-call rotation for major services when further support is necessary.

VigiLife uses a security agent to monitor production systems. The agents monitor system activities, generate alerts on suspicious activities and report on vulnerability findings to a centralized management console.

The security agent is installed on all on premise Linux servers. It is also built into Amazon Machine Images (AMIs) for use in VigiLife AWS environments.

Protecting Data At Rest

Encryption of Data at Rest

All databases, data stores, and file systems are encrypted with AES-256 encryption.

Local Disk/Volume Encryption

Encryption and key management for local disk encryption of on-premise servers and end-user devices follow the defined best practices for Windows, macOS, and Linux/Unix operating systems.

Protecting Data In Transit

1. All external data transmission is encrypted end-to-end using encryption keys managed by VigiLife. This includes, but is not limited to, cloud infrastructure and third party vendors and applications.
2. Transmission encryption keys and systems that generate keys are protected from unauthorized access. Transmission encryption key materials are protected with access controls, and may only be accessed by privileged accounts.
3. Transmission encryption keys use a minimum of 2048-bit RSA keys, or keys and ciphers of equivalent or higher cryptographic strength (e.g., 256-bit AES session keys in the case of IPSec encryption).
4. Transmission encryption keys are limited to use for one year and then must be regenerated.
5. For all VigiLife APIs, enforcement of authentication, authorization, and auditing is used for all remote systems sending, receiving, or storing data.
6. System logs of all transmissions of Production Data access are kept. These logs must be available for audit.

Encryption of Data in Transit

All internet and intranet connections are encrypted and authenticated using TLS 1.2.

Data protection via end-user messaging channels

Restricted and sensitive data is not allowed to be sent over electronic end-user messaging channels such as email or chat, unless end-to-end encryption is enabled.

Protecting Data In Use

Data in Use, sometimes known as Data in Process, refers to active data being processed by systems and applications which is typically stored in a non-persistent digital state such as in computer random-access memory (RAM), CPU caches, or CPU registers.

Protection of data in use relies on application layer controls and system access controls. See the [Production Security / SDLC][1] and [Access][2] sections for details. [1] :/sdlc/ [2] :/access/

VigiLife applications implement logical account-level data segregation to protect data in a multi-tenancy deployment. In addition, VigiLife applications may incorporate advanced security features such as Attribute Based Access Control (ABAC) for protection of data in use.

Encryption Key Management

VigiLife uses AWS Key Management Service (KMS) for encryption key management.

Certificate Management

VigiLife uses AWS Certificate Manager (ACM) for certificate management.

- Certificates are renewed automatically.
- Certificates are revocated if the certificate is no longer needed or upon discovery of potential compromise.

Data Integrity Protection

When appropriate, VigiLife engineering should implement "Versioning" and "Lifecycle", or equivalent data management mechanism, such that direct edit and delete actions are not allowed on the data to prevent accidental or malicious overwrite. This protects against human errors and cyberattacks such as ransomware.

- All edits create a new version and old versions are preserved for a period of time defined in the lifecycle policy.

Additionally, all access to sensitive data is authenticated, and audited via logging of the infrastructure, systems and/or application.

Secure Software Development and Product Security

2024.02.13

VigiLife development team follows the latest security best practices when developing software, and automates security testing throughout development lifecycle whenever possible.

Security is integrated into all phases of VigiLife product development lifecycle, including:

- Secure Design:
    - App Risk classification
    - Security req definition
    - Secure application design / RFC
    - Threat modeling
    - App data flow analysis
- Secure Development and Testing:
    - Secure coding guidelines
    - Peer review

- Peer review
    - Security testing, for example:
        - Linting with security rules
        - Open source security analysis
        - Static secure code analysis
        - Dynamic security analysis
        - Penetration testing
    - Responsible vulnerability disclosure / bug bounty program
- Remediation:
    - Follows defined vulnerability management lifecycle
    - Ensures no high risk security vulnerability is in production

Details about the VigiLife software application architecture and security are documented on the product development / engineering wiki.

Policy Statements

VigiLife policy requires that:

(a) VigiLife software engineering and product development is required to follow security best practices. Product should be "Secure by Design" and "Secure by Default".

(b) Quality assurance activities must be performed. This may include

- peer code reviews prior to merging new code into the main development branch (e.g. master branch); and
- thorough product testing before releasing to production (e.g. unit testing and integration testing).

(c) Risk assessment activities (i.e. threat modeling) must be performed for a new product or major changes to an existing product.

(d) Security requirements must be defined, tracked, and implemented.

(e) Security analysis must be performed for any open source software and/or third-party components and dependencies included in VigiLife software products.

(f) Static application security testing (SAST) must be performed throughout development and prior to each release.

(g) Dynamic application security testing (DAST) must be performed prior to each release.

(h) All critical or high severity security findings must be remediated prior to each release.

(i) All critical or high severity vulnerabilities discovered post release must be remediated in the next release or within the defined, predetermined timeframe.

(j) Any exception to the remediation of a finding must be documented and approved by the security team.

Controls & Procedures

Software Development Process
Overview

Software development at VigiLife follows a release strategy that provides traceability for production software changes. Features, enhancements, and bugs are written up as Issues in GitHub Issues. An engineer on a small team proposes changes necessary and creates a review for the team (GitHub). Continuous integration (GitHub Actions) kicks off unit and functional tests which pass before changes are merged into the repository. Once the review is complete, the changes are now deployed to the development environment where regression and end-to-end tests are run before the new code replaces the existing in-service code (test then deploy model).

VigiLife practices continuous delivery of code into production through multiple environments: development, staging, production. The deploy process and infrastructure roll-out are written as code (using technologies such as AWS Cloudformation) and managed under source control.

VigiLife's multiple lower environments (e.g. development) provide an ecosystem of sample data sets that exercise the application and services when test automation is run. Performance and scalability changes are driven by metric data captured through monitoring and

logging (metrics before and after change – typically captured as part of the issue description/writeup).

Deployments to production are gated by change control process where an issue is opened which identify what is new/changed (GitHub Issues). Sign-offs are recorded by development, testing, security, and product management. Production roll-outs happen on a regular basis without impact to service. This continuous process allows for security updates to roll out regularly and with urgency. If there is impact to production, a rollback is performed to restore service and whatever caused the problem is reverted from source. This restarts the re-proposal approval process of source changes. This process keeps the set of differences between the development environment and the

production environment as low as possible.

Secure Development Standards

Traceability of code changes allow for our software to be a living entity. Our current system for documenting changes is GitHub Issues. Every commit and/or Pull-Request, should have a GitHub Issues supplied that describes contextually why this change is necessary and reasonable. These artifacts over time allow for one to trace the lineage of why our production software and services change over time.

All VigiLife git repositories have a company standard configuration from a GitHub perspective. This standard is a guideline and can be relaxed, but socialize when those exceptions are needed. One example of an exception, is the wiki repository, as editing a wiki and always requiring a PR in this setting slows down 'flow'.

- Code: <#>
- Repo settings: <#>
- Build: <#>

NOTE: The Sandbox project (and repos) do not follow this standard. And certain projects might be excluded (e.g. wiki).

Developers follow the branch strategy and code review process below:

1. All development uses feature branches based on the main branch used for the current release. Any changes required for a new feature or defect fix are committed to that feature branch.
    - These changes must be covered under 1) a unit test where possible, or 2) integration tests.
    - Integration tests are *required* if unit tests cannot reliably exercise all facets of the change.
2. Once the feature and corresponding tests are complete, a pull request (PR) will be created using the GitHub. The pull request should indicate which feature or defect is being addressed and should provide a high-level description of the changes made.
3. Code reviews are performed as part of the pull request procedure. Once a change is ready for review, the author(s) will notify other engineers using an appropriate mechanism, typically by adding reviewers as PR approvers.
    - Other engineers will review the changes, using the guidelines above.
    - Engineers should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.
    - If changes/commits are made to a PR, it should reset previous approvals and require review and approvals again before the PR can be merged.
    - Once the review process finishes, each reviewer should approve the PR, at which point the original author(s) may merge their change into the main branch (i.e. main).
    - PR can only be merged with at least one approval from a reviewer other than the author.
4. If the feature or defect interacts with sensitive data, or controls access to sensitive data, or contains security/risky infrastructure changes to the target environment, the code changes must be reviewed by the Security team before the feature is marked as complete.
    - This review must include a security analysis for potential vulnerabilities such as those listed in the OWASP Top 10.
    - This review must also verify that any actions performed by authenticated users will generate appropriate audit log entries.

Detailed process and procedures for code promotion and production release: See Configuration and Change Management.

Source Code Management

VigiLife development/engineering team uses GitHub for source code management. Access to GitHub and its configuration standards include:

- All developers must authenticate to gain access to GitHub and code repos hosted on GitHub according to standards and procedures defined in the Access Policy:
    - Access control to the GitHub web interface must be enabled, via SSO and/or MFA if applicable
    - SSH public/private key access may be used for command line or git access to the code repos
- All code repos in GitHub follow these configuration standards:
    - All repos must have an owner identified and listed
    - All repos are by default private
- Certain branch restrictions are enabled, including:
    - The main branch cannot be rebased
    - Restrict direct commits into main

    - Restrict history rewrites of main
    - Restrict deletion of main
- Certain pull request (PR) requirements are enforced before merging, including:
    - Must have at least 1 review approval to merge
    - Must have at least 1 successful build to merge
    - all PR tasks must be completed

High Level Application Security Requirements

All VigiLife software must be developed to include the following general application security principles and requirements. Web applications must also protect itself against the OWASP Top 10 vulnerabilities.

1. Protect sensitive customer data such as PHI, PII and account passwords. Encrypt data stored (at rest).
2. Secure data in transit and customer communications via TLS.
3. Provision strong access control (authentication and authorization). Prevent and report unauthorized access.
4. Log all transactions and activities to be able to tell who did what, when, where, and how. Mask or remove sensitive data in logs.
5. Implement client security at application endpoints (e.g. browser, mobile app).
6. Communicate securely across application endpoints and between service consumers/producers.
7. Use secure defaults to ensure security when in all error conditions.
8. Check and maintain the security of all third party and open source libraries/components/dependencies.
9. Validate all data inputs; encode data outputs when appropriate.
10. Deploy and configure applications securely to production.
11. Perform regular vulnerability analysis and apply security patches promptly.
12. Secure privileged access to production environments and ensure ongoing application monitoring.

All software code must complete a set of security scans/testing prior to being deployed to production, including open source dependency scanning, static and dynamic application security testing, as well as periodic penetration testing.

Pre-production testing is performed with nonproduction data in nonproduction environments. Health checks are performed regularly or automated in production.

Software vulnerability identified through any of the above processes shall be reported and tracked following VigiLife Vulnerability Management process as defined in the Vulnerability Management Policy and Procedures.

Secure Design and Application Threat Modeling

VigiLife Security Team in collaboration with development team performs full Application Threat Modeling and Risk Assessment on per-

application basis using a custom approach that relies on industry standards and best practices.

Major application updates are captured via an **RFC** process. The RFC template includes **Security Consideration** as a required section. This section is used to document abuse cases including:

- risks identified,
- attack vectors, and
- mitigating controls.

Each RFC is required to capture sufficient details of the feature/component to be developed, including use cases, motivation and outcome, and the following design details as applicable:

- authentication/authorization mechanisms,
- network communications,
- data encryption,

- cloud services used,
- logging/auditing,
- data flow diagram/description,
- edge cases, drawbacks, and alternatives.

The RFC must be approved prior to implementation. Security team is included in RFC reviews via the pull request process.

Platform Design and DevOps Security Details

Platform Design and DevOps Security Details

Documentation on the VigiLife Engineering Wiki may include additional security specifications as well as the security design and implementation details of the VigiLife Platform and its supporting operations.

Access Control of the Application (Identification, Authentication, Authorization, Accounting)

VigiLife external software application that is customer facing with access to customer specific data, including sensitive information such as PII and ePHI, implements strong access control, covering the Identification, Authentication, Authorization, and Accounting/Auditing (IAAA) of access and user activity.

The implementation ensures that

- the user requesting access is the one claimed (Identification and Authentication);
- only users authorized to access specific data (such as ePHI) are allowed to (Authorization); and
- their access activities are logs (Accounting/Auditing) according to the VigiLife auditing standards.

The backend platform implements granular Attribute-Based Access Control (ABAC) for granting access to specific services and data based on the attribute(s) of a principal (i.e. user requesting access -- an attribute could be the role or group membership or organization the user belongs to) and the attribute(s) of the requested resource (i.e. data or service -- an attribute could be the project this data belongs to).

More implementation details are documented on the internal Engineering wiki.

Free and Open Source Software (FOSS) Security

VigiLife security and development team implemented a process to

- Inventory all software dependencies;
- Scan software dependencies for known security vulnerability;
- Fix any and all high risk findings
- Review and identify licensing issues of the 3rd party software and libraries.

The current tool in use is . Documentation can be found at the website.

Static Application Security Testing (SAST)

is the standard service used to perform static analysis of all code bases. When SonarCloud is unable to be used, robust linting tools must be used. All tools must be run with CI jobs, and should fail the CI job if there is a finding. Any finding that is discovered should be reported in GitHub Issues and remediated as soon as possible to prevent future jobs from failing.

Dynamic Application Security Testing (DAST)

Dynamic testing is available by request to the Security team and is performed using . Security team is currently looking into automation of this type of scanning via GitHub Actions

Additionally, manual baseline dynamic testing is available by request to the Security team.

Penetration Testing

External Penetration Testing

An external penetration testing is performed at least once a year by a qualified security researcher / ethical hacker on the security team internally and/or with an external security consulting firm.

Outsourced Software Development

VigiLife requires all outsourced software development to follow the same rigor and process as internal engineering. Outsourced developers must develop in our secure environment, accept and follow our security policies and procedures, and comply with the same secure coding standards, including:

- Receive regular OWASP or equivalent secure coding training.
- Follow the same source control, code review, and security code scanning procedures as defined.
- Install endpoint compliance agent that checks to make sure firewall, encryption, patching, password policy, screensaver password, and other required protection is properly configured.

Additionally, the third party firm providing outsourced development services must demonstrate that they have conducted the appropriate screening during hiring.

HIPAA Best Practices for Software Development

Use only HIPAA eligible services in the Cloud (AWS)

Because we use the services provided by AWS for our production environment with contains electronic protected health information (ePHI), AWS is a "business associate" of ours. It is required by HIPAA for VigiLife and AWS to enter into a ["business associate agreement" (BAA)] [BAA].

[BAA] : https://aws.amazon.com/blogs/security/tag/aws-business-associate-agreement/

Our fully executed BAA with AWS can be found on the internal document repository.

We must only used HIPAA-eligible services covered under the BAA to process and store ePHI. Non-eligible services may be used in support of our cloud infrastructure as long as it does not have access to ePHI.

A list of HIPAA eligible services can be found here. AWS regularly updates its services to meet HIPAA compliance requirements. Check the page once in a while to find out if new services have been added.

Additional References:

- Architecting for HIPAA in the Cloud
- AWS Shared Responsibility Model
- AWS HIPAA Compliance
- AWS HIPAA Compliance Whitepaper

Separate access and data between prod and non-prod accounts

It is a compliance requirement of multiple regulations to ensure separation of duties between production and non-production environments, including both access and data. Additionally, we should not use production data for dev or test, unless the data has been properly sanitized/masked.

Examples of regulations and certifications that have this explicit requirement include HIPAA, SAS70/SSAE-17, SOC, PCI, and ISO 27001/27002, many of which are on our target list to be compliant with or certified to.

Do not log ePHI

Not only it is a security best practice to avoid sensitive data such as ePHI in application logging, it may be a contract violation (per AWS BAA) to do so. We must not send any ePHI to non HIPAA eligible services in AWS, such as CloudTrail.

Include the right language in notices

Specific language must be included in terms, consents, and notices. For example, we must collect email addresses from patients when they sign up for the PHC, and specify in the terms that we may use the email address provided as a formal method of communication, including breach notification, should a breach occurs that impact their PHI.

Data protection

Follow the requirements listed in the following documents:

- Data Classification Model;
- Data Handling Requirements;
- Data Protection Policy and Procedures; and
- Backup and Recovery Process.

Production System Monitoring and Paging

Software and systems deployed in production are monitored 24/7 for health check and other major/critical error conditions. When alarms are triggered, notifications are sent to Slack on a pre-configured channel which are reviewed and triaged by the response team.

Configuration and Change Management

2024.04.17

VigiLife standardizes and automates configuration management through the use of automation scripts as well as documentation of all

changes to production systems and networks. Automation tools (e.g. CloudFormation) automatically configure all VigiLife systems according to established and tested policies, and are used as part of our Disaster Recovery plan and process.

Policy Statements

VigiLife policy requires that:

(a) All production infrastructure must be invoked through approved change management process.

(b) Each production change must maintain complete traceability to fully document the request, including requestor, date/time of change, actions taken and results.

(c) Each production change must be fully tested prior to implementation.

(d) Each production change must include a rollback plan to back out the change in the event of failure.

(e) Each production change must include proper approval.

- The approvers are determined based on the type of change.
- Approvers must be someone other than the author/executor of the change.
- Approvals may be automatically granted if certain criteria is met. The auto-approval criteria must be pre-approved by the Security Officer and fully documented and validated for each request.

Controls & Procedures

Configuration Management Processes

1. Configuration management is automated using industry-recognized tools CloudFormation
2. All changes to production systems, network devices, and firewalls are reviewed and approved before they are implemented to assure they comply with business and security requirements.
3. All changes to production systems are tested before they are implemented in production.
4. Implementation of approved changes are only performed by authorized personnel.
5. Tooling is used to generate an up to date system inventory.
    - All systems are categorized and labeled by their corresponding environment, such as *dev*, *test*, and *prod*.
    - All systems are classified and labeled based on the data they store or process, according to VigiLife data classification model.
    - The Security team maintains automation which monitors all changes to IT assets, generates inventory lists, using automatic IT assets discovery, and services provided by each cloud provider.
    - IT assets database is used to generate the diagrams and asset lists required by the Risk Assessment phase of VigiLife's Risk Management procedures
    - VigiLife Change Management process ensures that all asset inventory created by automation is reconciled against real changes to production systems. This process includes periodic manual audits and approvals.
    - During each change implementation, the change is reviewed and verified by the target asset owner as needed.
6. All frontend functionality (e.g. user dashboards and portals) is separated from backend (e.g. database and app servers) systems by being deployed as static webcontent via S3 and CloudFront.
7. All software and systems are required to complete full-scale testing before being promoted to production.
8. All code changes are reviewed to assure software code quality, while in development, to proactively detect potential security issues using pull-requests and static code analysis tools.

Configuration Monitoring and Auditing

All infrastructure and system configurations, including all software-defined sources, are centrally aggregated to a configuration management database (CMDB) -- .

Configuration auditing rules are created according to established baseline, approved configuration standards and control policies. Deviations, misconfigurations, or configuration drifts are detected by these rules and alerted to the security team.

Production Systems Provisioning

1. Provisioning request must be approved before any new system can be provisioned, unless a pre-approved automation process is followed. By default this is done via Pull Request (PR) Review in Github
2. If the system will be used to store sensitive information, the implementer must ensure the volume containing this sensitive data is encrypted.

3. Sensitive data in motion must always be encrypted.
4. A security analysis is conducted once the system has been provisioned. This can be achieved either via automated configuration/vulnerability scans or manual inspection by the security team. Verifications include, but is not limited to:
    - Removal of default users used during provisioning.
    - Network configuration for system.
    - Data volume encryption settings.
    - Intrusion detection and virus scanning software installed.
5. The new system is fully promoted into production upon successful verification against corresponding VigiLife standards and change request approvals.

User Endpoint Security Controls and Configuration

1. Employee laptops, including Windows, Mac, and Linux systems, are configured either
    - Manually by IT or the device owner; or
    - Automatically using a configuration management tool or equivalent scripts.
2. The following security controls are applied at the minimum:
    - Disk encryption
    - Unique user accounts and strong passwords
    - Approved security agents
    - Locking after 2 mins of inactivity
    - Auto-update of security patches
3. The security configurations on all end-user systems are inspected by Security through either a manual periodic review or an automated compliance auditing tool.

Configuration and Provisioning of Management Systems

1. Provisioning management systems such as configuration management servers, remote access infrastructure, directory services, or monitoring systems follows the same procedure as provisioning a production system.
2. Critical infrastructure roles applied to new systems must be clearly documented by the implementer in the change request.

Configuration and Management of Network Controls

All network devices and controls on a sensitive network are configured such that:

- Vendor provided default configurations are modified securely, including
    - default encryption keys,
    - default SNMP community strings, if applicable,
    - default passwords/passphrases, and
    - other security-related vendor defaults, if applicable.
- Encryption keys and passwords are changed anytime anyone with knowledge of the keys or passwords leaves the company or changes positions.
- Traffic filtering (e.g. firewall rules) and inspection (e.g. Network IDS/IPS or AWS VPC flow logs) are enabled.
- An up-to-date network diagram is maintained.

In AWS, network controls are implemented using Virtual Private Clouds (VPCs) and Security Groups. The configurations are managed as code and stored in approved repos. All changes to the configuration follow the defined code review, change management and production deployment approval process.

Provisioning AWS Accounts

AWS Account Structure / Organization

VigiLife maintains a single Organization in AWS, maintained in a top-level AWS account (root). Sub-accounts are connected that each hosts separate workloads and resources in its own sandboxed environment. The master account itself handles aggregated billing for all connected sub-accounts but does not host any workload, service or resource, with the exception of DNS records for VigiLife root domain, using AWS Route53 service. DNS records for subdomains are maintained in the corresponding sub-accounts.

Access to each account is funneled through our designated SSO provider, which establishes a trust relationship to a set of predefined roles

Access to each account is funneled through our designated SSO provider, which establishes a trust relationship to a set of predefined roles in the master account. Once authenticated, a user then leverages AWS IAM Assume Role capability to switch to a sub-account to access services and resources.

Automated change management for deploys to AWS

VigiLife uses Infrastructure-as-code as a core component for managing cloud DevOps. This currently uses as the foundational service, and leverages other tools/languages such as SAM or CDK.

When deploying an infrastructure to production, the following processes should be taken:

1. Ensure the latest code from the desired branch has been checked out (e.g. main or hotfix), then create a tag for with the deployment version/info
2. Run necessary build tools to create deployment artifacts (e.g. `sam build`)
3. Begin deployment process using appropriate deployment tools (e.g. `sam deploy`), and ensure appropriate deployment variables are set correctly
4. Review pre-deployment change log to ensure these match expectations for the release
5. Confirm deployment and review deployment status until finished; if deployment fails, review the failure and if unable to resolve, report as an issue in

Patch Management Procedures

Local Systems

VigiLife uses automated tooling to ensure systems are up-to-date with the latest security patches.

- On local Linux and Windows systems, the unattended-upgrades tool is used to apply security patches in phases.
    - High Risk security patches are automatically applied as they are released
    - Monthly system patching for regular applications are applied as needed.
    - Snapshotting of a system will take place before an update is applied.
    - Once the update is deemed stable the snapshot will be removed.
    - In case of failure of the update the snapshot will be rolled back.
    - If the staging systems function properly after the two-week testing period, the security team will promote that snapshot into the mirror used by all production systems. These patches will be applied to all production systems during the next nightly patch run.
    - The patching process may be expedited by the Security team
    - On Windows systems, the baseline Group Policy setting configures Windows Update to implement the patching policy.

Cloud Resources

VigiLife follows a "cattle-vs-pets" methodology to keep the resources in the cloud environments immutable and up-to-date with security patches.

- All production computation uses AWS Lambda which supports epheremal computation and pre-approved runtimes
- AWS Lambdas are scanned for vulnerabilites using the managed service AWS Inspector

User Endpoints

VigiLife requires auto-update for security patches to be enabled for all user endpoints, including laptops and workstations.

- The auto-update configuration and update status on all end-user systems are inspected by Security through either manual periodic audits or automated compliance auditing agents installed on the endpoints.

Production Deploy / Code Promotion Processes

In order to promote changes into Production, a valid and approved Pull Request (PR) is required, which is created and managed in GitHub Issues.

- At least one approval is required for each PR. By default, this will be done by Lead Engineer or VP of Engineering
- Additional approver(s) may be added depending on the impacted component(s). For example,
    - the IT Manager is added as an approver for IT/network changes; and
    - the DevOps Lead is added as an approver for CI/CD changes

- Each PR requires the following information at a minimum:
    - Summary of the change
    - Component(s) impacted
    - Justification
    - Rollback plan
- Additional details are required for a code deploy, including:
    - Build job name
    - Build ID and/or number
    - Deploy action (e.g. plan, apply)
    - Deploy branch (e.g. main)
    - Target environment (e.g. VigiLife-prod)
    - Links to pull requests and/or GitHub Issues issues
    - Security scan status and results

Emergency Change

In the event of an emergency, the person or team on call is notified. This may include a combination or Development, IT, and Security.

If an emergency change must be made, such as patching of a zero-day security vulnerability or recovering from a system downtime, and that the standard change management process cannot be followed due to time constraint or personnel availability or other unforeseen issues, the change can be made by:

- **Notification:** The Engineering Lead, Security Lead, and/or IT Lead must be notified by email, Slack, or phone call prior to the change . Depending on the nature of the emergency, the leads may choose to inform members of the executive team.
- **Access and Execution:** Manually access of the production system or manual deploy of software, using one of the following access mechanisms as defined in Access Control policy and procedures:
    1. Support/Troubleshooting access
    2. Root account or root user access
    3. Local system access (for on-premise environment)
- **Post-emergency Documentation:** A ticket should be created within 24 hours following the emergency change. The ticket should contains all details related to the change, including:
    - Reason for emergency change
    - Method of emergency access used
    - Steps and details of the change that was made
    - Sign-off/approvals must be obtained per the type of change as defined by the standard CM process
- **Prevention and Improvement:** The change must be fully reviewed by Security and Engineering together with the person/team responsible for the change. Any process improvement and/or preventative measures should be documented and an implementation plan should be developed.

Threat Detection and Prevention

2024.02.13

In order to preserve the integrity of data that VigiLife stores, processes, or transmits for Customers, VigiLife implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. This include threat detection and prevention at both the network and host level, as well as threat intelligence monitoring.

Policy Statements

VigiLife policy requires that:

(a) All critical systems, assets and environments must implement realtime threat detection or prevention.

Controls & Procedures

System Malware Protection

1. All end-user workstations and production systems must have antivirus running. The default anti-malware solution used is . The anti-malware solution will include protection against malicious mobile code.
    - Next generation endpoint protection agent may be used as an equivalent solution.
    - Hosts are scanned continuously for malicious binaries in critical system paths. Additionally, if supported, the agent is set to to

scan system every 2 hours and at reboot to assure no malware is present.
    - The malware signature database is kept up to date, changes are pushed continuously.
    - Logs of virus scans and alerts are maintained according to the requirements outlined in System Auditing.
2. Detected malware is evaluated and removed following the established incident response process.
3. All systems are to only be used for VigiLife business needs.

Firewall Protection

Firewall protection is implemented at the following layers

- **Network** - including Network ACL and Security Groups in AWS as well as on- premise firewalls between the office networks and the Internet.
- **Host** - local firewalls are enabled on the user endpoints as well as servers (compute and database instances in AWS are protected by security groups)
- **Application** - web application firewall (WAF) and content distribution are configured at the application layer to protect against common web application attacks such as cross site scripting, injection and denial-of-service attacks.

Network Intrusion Detection

Intrusion Detection for On-Premise Internal Networks

- VigiLife leverages for network security of its on-premise environments.
- features stateful firewall inspection and intrusion detection/prevention (IDS/IPS) of applicable incoming and outgoing network traffic. Attacks and suspicious network activities are blocked automatically.
- VigiLife IT manager is responsible for configuring the firewall and IDS/IPS rules and review the configuration as least quarterly.

Intrusion Detection in AWS Cloud Environments

VigiLife implemented a real-time threat detection solution by monitoring AWS Cloudtrail events and/or VPC flow logs.

- Cloudtrail events are monitored by ****
- VPC flow logs are sent to and analyzed by ****.

Additional monitoring is provided by our infrastructure service provider AWS.

Host Intrusion Detection

Host based intrusion detection is supported via one of the following:

- On Windows and macOS systems: **** agents for malware detection and behavior-based endpoint threat detection.
- On Linux servers: **** agents for activity monitoring, vulnerability scanning, and threat detection. This includes all virtual instances running in the cloud environment.

Web Application Protection

leverages AWS Services to protect web applications against common attacks such as SQL injection, cross-site scripting, and denial-of-service (DoS/DDoS) attacks. The services used include AWS Shield, WAF, Cloudfront, and/or API Gateway.

Centralized Security Information and Event Management

Security events and alerts are aggregated to and correlated by one or both of the following solutions:

-
- Internally developed security automation tooling

Threat Intelligence Monitoring

NH-ISAC

VigiLife is an active member of the National Health Information Sharing and Analysis Center (NH-ISAC).

VigiLife Security team is subscribed to receive threat alerts from NH-ISAC.

Intelligence Feeds

Additional intelligence feeds are received automatically through some of the 3rd party security solutions that have been implemented on the networks and/or endpoints. The data gathered through these external intel feeds is automatically used by the security solutions to analyze events and generate alerts.

Regulatory Requirements Updates

The Security and Privacy Officer actively monitors the regulatory compliance landscape for updates to regulations such as HIPAA, PCI and GDPR.

Vulnerability Management

2024.02.13

Policy Statements

VigiLife policy requires that:

(a) All product systems must be scanned for vulnerability on the defined, predetermined schedule and with each major change, as applicable.

(b) All vulnerability findings must be reported and tracked to resolution. Records of findings must be retained for a defined, predetermined timeframe.

Controls & Procedures

Vulnerability Scanning and Infrastructure Security Testing

The scanning and identification of system vulnerabilities is performed by

1. Automated security agent installed on all Linux servers.
    - This includes physical and virtual servers hosted on premise as well as EC2 instances in AWS.
    - The agent automatically reports to a centralized management server/dashboard with details of the server instance and any vulnerability finding.
    - This assessment is performed on an ongoing basis.
2. Additionally, periodic security scans of VigiLife on-premise systems are done using a combination of open-source and commercial vulnerability testing tools, including:
    - OpenVAS
    - Nmap
    - OWASP ZAP
    - Burp Suite Pro
3. Penetration testing is performed regularly as part of the VigiLife vulnerability management policy.
    - External penetration testing is performed continuously through a public vulnerability disclosure / bug bounty program.
    - Additional external penetration testing is performed at least annually by either a certified penetration tester on VigiLife security team or an independent third party.
    - White-box internal penetration testing is performed at least quarterly by the security team.
4. VigiLife developed an internal vulnerability management tool/database used to track all system entities and associated vulnerabilities.
5. Findings from a vulnerability scan or penetration testing are analyzed by the security team, together with IT and Engineering as needed, and reported following the process as defined in the next section. A written report may be generated in addition to creating the findings in GitHub Issues.
6. All security testing reports and findings records are retained for 7 years.

Security Findings Reporting, Tracking and Remediation

We follow a simple vulnerability tracking process using GitHub Issues. The records of findings are retained for seven years.

Reporting a finding

Reporting a finding

- Upon identification of a vulnerability (including vulnerability in software, system, or process), a GitHub Issues Issue of (issueType = **Finding**) is created on the SECURITY Project.
- Populate the following custom fields as part of the GitHub Issues issue when applicable:
    - **Source of Finding** (dropdown list)
    - **In Production** (yes/no/na selection)
    - **Application/Repo Name** (text/tag)
    - **Version Number** (text/tag)
- The **Summary** of the Finding should be in this format: "{[sev]} {short description}" (e.g. "[High] Outdated package on ECS AMI image").
- The **Description** of the Finding should include further details, without any confidential information, and a link to the source.
- The **Priority** of the Finding should match its severity level.

Priority/Severity Ratings and Service Level Agreements

In an effort to quickly remediate security vulnerabilities the following timelines have been put in place to drive resolution.

Sev Rating	Priority Level	SLA	Definition	Examples
P0	Highest	48 hours	Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, unauthorized access to/extraction of sensitive data, etc.	Vulnerabilities that result in Remote Code Execution such as Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass
P1	High	30 days	Vulnerabilities that affect the security of the platform including the processes it supports.	Lateral authentication bypass, Stored XSS, some CSRF depending on impact.
P2	Medium	90 days	Vulnerabilities that affect multiple users, and require little or no user interaction to trigger.	Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact.
P3	Low	Best Effort	Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger.	Common flaws, Debug information, Mixed Content.

In the case a sev rating / priority level is updated after a vulnerability finding was originally created, the SLA is updated as follow:

- **severity upgrade:** reset SLA from time of escalation
- **severity downgrade:** SLA time remains the same from time of creation/identification of finding

Resolving a finding

- The Finding should be assigned to the owner responsible for the system or software package.
- All findings should be addressed according to the established SLA.
- No software should be deployed to production with unresolved HIGH or MEDIUM findings, unless an Exception is in place (see below).
- A finding may be resolved by
    1. providing a valid fix/mitigation
    2. determining as a false positive
    3. documenting an approved exception

Closing a finding

- The assignee should provide a valid resolution (see above) and add a comment to the finding.
- The finding should be re-assigned to the Reporter or a member of the security team for validation.
- Upon validation, the finding can be marked as Done (closed) by the Reporter.
- **Before the finding can be marked as closed by the reporter, the fix must be deployed to dev and have a targeted release date for deploying to production noted on the ticket.**

Exceptions

- An Exception may be requested when a viable or direct fix to a vulnerability is not available. For example, a version of the package that contains the fix is not supported on the particular operating system in use.
- An alternative solution (a.k.a. compensating control) must be in place to address the original vulnerability such that the risk is mitigated. The compensating control may be technical or a process or a combination of both.

- An Exception must be opened in the form of a GitHub Issues issue (issueType = **Exception**) on the SECURITY project.
- The Exception GitHub Issues issue must reference the original Finding by adding an Issue Link to the Finding GitHub Issues issue.
- Each Exception must be reviewed and approved by the Security team and the impacted asset owner.
- All Exceptions are reviewed every six months to re-assess its validity.

Mobile Device Security and Storage Media Management

2024.02.13

VigiLife recognizes that media containing sensitive data may be reused when appropriate steps are taken to ensure that all stored sensitive data has been effectively rendered inaccessible. Destruction/disposal of sensitive data shall be carried out in accordance with federal and state law. The schedule for destruction/disposal shall be suspended for sensitive data involved in any open investigation, audit, or litigation.

VigiLife utilizes virtual storage repositories to store production data. Volumes and repositories utilized by VigiLife and VigiLife Customers are encrypted. VigiLife does not use, own, or manage any mobile devices, removable storage media, or backup tapes that have access to sensitive data.

Policy Statements

VigiLife policy requires that:

(a) All media, including mobile and removable media, storing VigiLife company data must be encrypted.

(b) Critical data as defined in VigiLife data classification model §data-management may not be stored on mobile devices or removable media such as USB flash drives.

(c) All destruction/disposal of sensitive data storage media will be done in accordance with federal and state laws and regulations and pursuant to the VigiLife's written retention policy/schedule.

- Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed of.

(d) All sensitive data must rendered inaccessible in a forensically sound manner prior to media reuse or disposal.

(e) Mobile devices, including laptops, smart phones and tables, used in support of critical business operations shall be fully managed and/or audited by VigiLife IT and Security.

Controls & Procedures

Media Disposal Process

IT and Security is responsible to ensure media containing critical / sensitive data is disposed securely in the following manner:

- The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services. This may include
    - Secure wipe;
    - Physical destruction;
    - Destruction of encryption keys (if the data on the media is encrypted using a strong algorithm such as AES-256).
- If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- All VigiLife Subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all patient health information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
- In the cases of a VigiLife Customer terminating a contract with VigiLife and no longer utilize VigiLife Services, data will be returned or disposed per contract agreement or VigiLife Platform use terms and conditions. In all cases it is solely the responsibility of the VigiLife Customer to maintain the safeguards required of laws and regulations once the data is transmitted out of VigiLife environments.

Use of USB Flash Drive and External Storage Device

Per VigiLife corporate policy, confidential and critical data may not be stored on external devices such as USB flash drives. This includes and is not limited to ePHI. For definition of confidential and critical data, see VigiLife Data Classification and Handling Policy.

is not limited to: PII. For definition of confidential and critical data, see VigiLife Data Classification and Handling Policy.

Usage of USB flash drives for temporary transfer of confidential and critical data may be allowed on a case by case basis, when the following process is followed:

- Data is only allowed on encrypted flash devices approved by VigiLife Security and the IT Manager (currently ****).
- The process starts with the submission of a ticket in GitHub Issues. The ticket must be approved by IT and Security.
- Upon completion of data transfer all sensitive data on the device must be completely removed.
- The device is to be returned to the IT Manager to double check that the data has been removed.
- The IT Manager will check the drive back in.

Management of BYOD Devices

VigiLife provides company-issued laptops and workstations to all employees.

Mobile devices (including phones and personal smart devices) may NOT be used for business purpoose under any conditions.

Business Continuity and Disaster Recovery

2024.02.13

The VigiLife Contingency Plan establishes procedures to recover VigiLife following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the VigiLife Security Officer and Privacy Officer.

HIPAA: This VigiLife Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

NIST: This VigiLife Contingency Plan is created under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.

Policy Statements

VigiLife policy requires that:

(a) A plan and process for business continuity and disaster recovery (BCDR), including the backup and recovery of systems and data, must be defined and documented.

(b) BCDR shall be simulated and tested at least once a year. Metrics shall be measured and identified recovery enhancements shall be filed to improve the BCDR process.

(c) Security controls and requirements must be maintained during all BCDR activities.

Controls & Procedures

BCDR Objectives and Roles
Objectives

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - *Notification/Activation phase* to detect and assess damage and to activate the plan;
    - *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
    - *Reconstitution phase* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out VigiLife processing requirements during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to VigiLife systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering VigiLife during prolonged periods of interruption to normal operations.
5. Ensure coordination with other VigiLife staff who will participate in the contingency planning strategies.

6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, and internal malicious activities.

VigiLife defined two categories of systems from a disaster recovery perspective.

1. *Critical Systems*. These systems host production application servers/services and database servers/services or are required for functioning of systems that host production applications and data. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.
2. *Non-critical Systems*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Line of Succession

The following order of succession to ensure that decision-making authority for the VigiLife Contingency Plan is uninterrupted. The Chief Operating Officer (COO) is responsible for ensuring the safety of personnel and the execution of procedures documented within this VigiLife Contingency Plan. The Head of Engineering is responsible for the recovery of VigiLife technical environments. If the COO or Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO shall function as that authority or choose an alternative delegate. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

- Roger Edwards, COO: roger.edwards@vigilife.com
- Noah DePriest, Head of Engineering: noah.depriest@vigilife.com
- Zachary Kiehl, CEO: zachary.kiehl@vigilife.com

Response Teams and Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting VigiLife infrastructure and systems.

1. **IT** is responsible for recovery of the VigiLife hosted environment, network devices, and all servers. The team includes personnel responsible for the daily IT operations and maintenance. The team leader is the IT Manager who reports to the COO.
2. **HR & Facilities** is responsible for ensuring the physical safety of all VigiLife personnel and environmental safety at each VigiLife physical location. The team members also include site leads at each VigiLife work site. The team leader is the Facilities Manager who reports to the COO.
3. **DevOps** is responsible for assuring all applications, web services, platform and their supporting infrastructure in the Cloud. The team is also responsible for testing re-deployments and assessing damage to the environment. The team leader is the Head of Engineering.
4. **Security** is responsible for assessing and responding to all cybersecurity related incidents according to VigiLife Incident Response policy and procedures. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer.

Members of above teams must maintain local copies of the contact information of the BCDR succession team. Additionally, the team leads must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

All executive leadership shall be informed of any and all contingency events. Current members of VigiLife leadership team include the CEO, VP of Engineering, VP of Product & Partnerships, VP of Security.

General Disaster Recovery Procedures

Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to VigiLife. Based on the assessment of the Event, sometimes according to the VigiLife Incident Response Policy, the Contingency Plan may be activated by either the COO or Head of Engineering. The Contingency Plan may also be activated by the Security Officer in the event of a cyber disaster.

The notification sequence is listed below:

- The first responder is to notify the COO. All known information must be relayed to the COO.
- The COO is to contact the Response Teams and inform them of the event. The COO or delegate is responsible to begin assessment procedures.
- The COO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the COO is to following the steps below.
    - Damage Assessment Procedures:
    - The COO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.

    - Alternate Assessment Procedures:
    - Upon notification, the COO is to follow the procedures for damage assessment with the Response Teams.

- The VigiLife Contingency Plan is to be activated if one or more of the following criteria are met:

    - VigiLife will be unavailable for more than 48 hours.
    - On-premise hosting facility or cloud infrastructure service is damaged and will be unavailable for more than 24 hours.
    - Other criteria, as appropriate and as defined by VigiLife.

- If the plan is to be activated, the COO is to notify and inform team members of the details of the event and if relocation is required.

- Upon notification from the COO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

- The COO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

- The COO is to notify remaining personnel and executive leadership on the general status of the incident.

- Notification can be message, email, or phone.

Recovery Phase

This section provides procedures for recovering VigiLife infrastructure and operations at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild VigiLife infrastructure to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected to begin initial communication - DevOps
2. Assess damage to the environment - DevOps
3. Create a new production environment using new environment bootstrap automation - DevOps
4. Ensure secure access to the new environment - Security
5. Begin code deployment and data replication using pre-established automation - DevOps
6. Test new environment and applications using pre-written tests - DevOps
7. Test logging, security, and alerting functionality - DevOps and Security
8. Assure systems and applications are appropriately patched and up to date - DevOps
9. Update DNS and other necessary records to point to new environment - DevOps
10. Update Partners and Customers affected through established channels - DevOps

Reconstitution Phase

This section discusses activities necessary for restoring full VigiLife operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. If necessary, when the hosted data center at the original or new site has been restored, VigiLife operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

1. Original or New Site Restoration

    - Repeat steps 5-9 in the Recovery Phase at the original or new site / environment.
    - Restoration of Original site is unnecessary for cloud environments, except when required for forensic purpose.

2. Plan Deactivation

    - If the VigiLife environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the VigiLife Media Disposal Policy.

Testing and Maintenance

The COO and/or Head of Engineering shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing.

Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

Tabletop Testing

Tabletop Testing is conducted in accordance with CMS's RMH Chapter 6 Supplemental Contingency Planning Exercise Procedures. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a

specific crisis.

Simulation and/or Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch compute and storage resources to alternate processing site.

Application Service Event Recovery

VigiLife will send emails to team owners to provide real time update and inform our customers of the status of each service. When significant status changes, new emails will be sent with details about an event that may cause service interruption / downtime.

A follow up root-cause analysis details (RCA) will be available to customers upon request after the event has transpired for further details to cause and remediation plan for the future. Event Service Level

Short (hours)

- Experience a short delay in service.
- VigiLife will monitor the event and determine course of action. Escalation may be required.

Moderate (days)

- Experience a modest delay in service where processes in flight may need to be restarted.
- VigiLife will monitor the event and determine course of action. Escalation may be required.
- VigiLife will notify customers of delay in service and provide updates on VigiLife's status page.

Long (a week or more)

- Experience a delay in service and processes in flight may need to be restarted.
- VigiLife will monitor the event and determine course of action. Escalation may be required.
- VigiLife will notify customers of delay in service and provide updates on VigiLife's status page.

Production Environments and Data Recovery

Production data is to be backed up in at least 2 AWS regions. VigiLife assumes that in the worst-case scenario, if one of the AWS regions in use in production goes down, it will failover to a functioning region and use the most recent production backup data to conitune operations. When the primary region is back online, VigiLife will work to migrate back to the primary region.

Recovery of production Environments and data should follow the procedures listed above and in Data Management - Backup and Recovery

Incident Response

2024.04.01

VigiLife implements an information security incident response process to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

The incident response process addresses:

- Continuous monitoring of threats through monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

Note

These policies were adapted from work by the [HIPAA Collaborative of Wisconsin Security Networking Group](http://hipaacow.org/wp-content/uploads/2015/02/HCR-Security-Incident-Response-

Policy Statements

VigiLife policy requires that:

(a) All computing environments and systems must be monitored in accordance to the policies and procedures specified in the following VigiLife policies and procedures:

- Auditing
- System Access
- End-user Computing and Acceptable Use

(b) All alerts must be reviewed to identify security incidents.

(c) Incident response procedures are invoked upon discovery of a valid security incident.

(d) Incident response team and management must comply with any additional requests by law enforcement in the event of criminal investigation or national security, including but not limited to warranted data requests, subpoenas, and breach notifications.

Controls & Procedures

Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) is responsible for:

- Review, analyze and log of all received reports and track their statuses.
- Performing investigations, creating and executing action plans, post-incident activities.
- Collaboration with law enforcement agencies.

Current members of the VigiLife SIRT:

- Security and Privacy Officer
- Head of Engineering

Incident Management Process

The VigiLife incident response process follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process.

VigiLife's incident response classifies security-related events into the following categories:

- **Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:
  - Hardware component failing causing service outages.
  - Software error causing service outages.
  - General network or system instability.
- **Precursors** - A sign that an incident may occur in the future. Examples:
  - Monitoring system showing unusual behavior.
  - Audit log alerts indicated several failed login attempts.
  - Suspicious emails targeting specific VigiLife staff members with administrative access to production systems.
  - Alerts raised from a security control source based on its monitoring policy
- **Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:
  - Alerts for modified system files or unusual system accesses.
  - Antivirus alerts for infected files or devices.
  - Excessive network traffic directed at unexpected geographic locations.
- **Incidents** - A confirmed attack / indicator of compromise or a validated violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:
  - Unauthorized disclosure of sensitive data.
  - Unauthorized change or destruction of sensitive data.
  - A data breach accomplished by an internal or external entity.
  - A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

VigiLife employees must report any unauthorized or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security team know about any observed precursors or indications as soon as they are discovered.

Attention

Incidents of a severity/impact rating higher than **MEDIUM** shall trigger the

following response process, or as defined more specifically in the **Incident Categories and Playbooks** section.

I - Identification and Triage

1. Immediately upon observation VigiLife members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways:
    1. Direct report to management, the Security Officer, Privacy Officer, or other;
    2. Email;
    3. Slack;
    4. Phone call;
2. The individual receiving the report facilitates the collection of additional information about the incident, as needed, and notifies the Security Officer (if not already done).
3. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.
    1. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.
        1. Non-Technical Event (minor infringement): the Security Officer of designee creates an appropriate issue in GitHub Issues and further investigates the incident as needed.
        2. Technical Event: Assign the issue to an technical resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a lack of resource or expertise in the area.
    2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior leadership by email.
        1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
        2. Once the investigation is completed, progress to Phase V, Follow-up.
        3. If the issue is a technical security incident, commence to Phase II: Containment.
        4. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
        5. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.
        6. The lead member of the SIRT team facilitates initiation of an Incident ticket in GitHub Issues Security Project and documents all findings and details in the ticket.
            - The intent of the Incident ticket is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
            - Each Incident ticket should contain sufficient details following the SANS Security Incident Forms templates, as appropriate.
4. The Security Officer, Privacy Officer, or VigiLife representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security and Privacy Officer.
5. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to VigiLife and potentially external.

II - Containment (Technical)

In this Phase, VigiLife's engineers and security team attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. Review any information that has been collected by the Security team or any other individual investigating the security incident.
2. Secure the blast radius (i.e. a physical or logical network perimeter or access zone).
3. Perform the following forensic analysis preparation, as needed:
    1. Securely connect to the affected system over a trusted connection.
    2. Retrieve any volatile data from the affected system.
    3. Determine the relative integrity and the appropriateness of backing the system up.
    4. As necessary, take a snapshot of the disk image for further forensic; and if appropriate, back up the system.
    5. Change the password(s) to the affected system(s).
    6. Determine whether it is safe to continue operations with the affect system(s).
    7. If it is safe, allow the system to continue to function; and move to Phase V, Post Incident Analysis and Follow-up.
    8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
    9. The individual completing this phase provides written communication to the SIRT.
4. Complete any documentation relative to the security incident containment on the Incident ticket, using SANS IH Containment Form as a template.

5. Continuously apprise Senior Management of progress.
6. Continue to notify affected Customers and Partners with relevant updates as needed.

III - Eradication (Technical)

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s).
2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
    1. An increase in network perimeter defenses.
    2. An increase in system monitoring defenses.
    3. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
    1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
4. Update the Incident ticket with Eradication details, using SANS IH Eradication Form as a template.
5. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
6. Apprise Senior Management of the progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase IV, Recovery.

IV - Recovery (Technical)

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

1. The technical team determines if the affected system(s) have been changed in any way.
    1. If they have, the technical team restores the system to its proper, intended functioning ("last known good").
    2. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
    3. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
    4. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
    5. Update the documentation with the detail that was determined during this phase.
    6. Apprise Senior Management of progress.
    7. Continue to notify affected Customers and Partners with relevant updates as needed.
    8. Move to Phase V, Follow-up.

V - Post-Incident Analysis (Technical and Non-Technical)

The Follow-up phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.
2. A "lessons learned" section is written and attached to Incident ticket.
    1. Evaluate the cost and impact of the security incident to VigiLife using the documents provided by the SIRT and the technical security resource.
    2. Determine what could be improved. This may include:
        - Systems and processes adjustments
        - Awareness training and documentation
        - Implementation of additional controls
    3. Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.
    4. Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.
3. Ensure all incident related information is recorded and retained as described in VigiLife Auditing requirements and Data Retention standards.

standards.

4. Close the security incident.

Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding the VigiLife's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

Incident Categories and Playbooks

- The IRT reviews and analyzes on the security events on as part of its daily operations.
- Based on the initial analysis, an event may be dismissed due to false positives, normal business operations, exceptions that are already in place, permitted per policy, or duplicates. An audit trail will be kept for event dismissal.
- A valid security event may be upgrade to a security incident. Upon which, an incident classification and severity is assigned as specified below.
- Record of the decision must be stored with details on date(s), name(s) of the person(s) conducted assessment.
- A containment, eradication and recovery procedure is triggered based on the Category classification of the incident.
- In addition to the general incident management procedures previously described, one or more of the following playbooks are consulted based on the classification of a particular incident.

Classification

- **Category 1** – General Incidents, including physical security incidents
- **Category 2** – Attacks on internal corporate infrastructure, including network, hardware, software
- **Category 3** – Malware
- **Category 4** – Attacks on external facing assets, such as website, web applications, web services. Including denial of service attacks.
- **Category 5** – Human targets, social engineering, phishing, etc.
- **Category 6** – Breach/leakage of critical or confidential data

Severity Levels:

- **Critical** – incident that involves immediate and significant interruption to business operations and/or breach of critical or confidential data
- **Major** – incident that involves immediate interruption to business operations but will not likely result in immediate data breach
- **Minor** – all other confirmed incidents

Response Procedures: Cat 1 – General Incident

- Prioritize handling the incident based on functional impact, informational effort, recoverability efforts and other relevant factors
- Report the incident to the appropriate internal personnel and external organizations
- Acquire, preserve, secure, and document evidence
- Contain the incident
- Eradicate the incident
    - Identify and mitigate all factors that enabled the incident to occur
    - Remove any results of malicious activity
- Recover from the incident
    - Restore affected systems and business functions
    - Implement additional preventive measures

Response Procedures: Cat 2 – Internal Infrastructure Incident Response

Depending on the type of event, use the following incident response playbooks:

- Unauthorized Access
- Root Access
- Elevation of Privilege
- Improper Usage

Response Procedures: Cat 3 – Malware outbreak

Depending on the agent type, follow these incident response playbooks:

- Malware
- Virus

Response Procedures: Cat 4 – External web attacks and DoS/DDoS attacks

- Mobilize the Engineering team to secure systems and ensure Business Continuity
- Conduct a thorough investigation of the incident
- Manage public relationships
- Address legal and regulatory requirements
- For a DDOS attack, follow the DDOS playbook
- Trigger BCDR if necessary

Response Procedures: Cat 5 – Social Engineering

Follow the Phishing incident response playbook

Response Procedures: Cat 6 – Data Leakage

Data Theft incident response playbook outlines the response instructions

Response Procedures: Special Cases

At least the following two special cases are considered when responding to an incident:

PHI/ePHI:

When a data breach occurs that involves unsecured PHI or ePHI, breach notifications must be performed according to HIPAA regulation requirements, including each individual impacted and as applicable, the covered entity and OCR (see Appendix for additional details).

If the breach or potential breach impacts PHI/ePHI that belongs to a Covered Entity to which VigiLife is a Business Associate of, the IRT and management team will inform the Covered Entity per the timeframe and contact method established in the Business Associate Agreement

or as described in §Breach Notification. HIPAA §164.410(b)

Criminal Activities:

In the event of an attack that involves suspected criminal activities, the IRT and management team will inform law enforcement.

Insider Threat:

Members of the cross-discipline insider threat incident handling team include:

- Security and Privacy Officer,
- COO, and
- Head of Engineering as appropriate.

Emergency Operations Mode

If an incident constitutes an emergency – for example, a detected cyberattack that impacts production systems – VigiLife plans to operate in a “read-only” request based mode, to continue to provide customers access to their data on request. All other access is temporarily blocked and data upload is paused until the emergency is resolved. This is accomplished by temporaril restricting all network traffic to APIs and web applications via WAF rules.

In emergency operations mode, temporary access may be granted to security and/or engineering team to access the production environments to perform forensics, root cause analysis, eradication/remediation, or other necessary activities for incident recovery.

Tabletop Exercise

At least once per year, VigiLife security and engineering teams jointly performs a Red Team exercise and/or a simulated "drill" of an emergency cyberattack that results in one or more **CRITICAL** incidents. Depending on the type of exercise, the duration may range from 2-4 hours (simulated "drill") to a couple of weeks (full Red Teaming exercise).

The exercise will follow a cyberattack playbook. It may be conducted with all internal resources or with the help of an external security consulting firm. The goal of the exercise is to ensure all parties involved receive proper training to handle an actual incident and to test out

the documented procedures in order to identify gaps ahead of a real event. Senior leadership team may be invited to participate in the "drill" depending on the nature of the exercise or receive a readout of the outcome.

Incident Tracking and Records

A record is created for each reported incident in . Each incident record contains details about the incident capturing the incident attributes and progression, including the following as applicable:

- Summary
- Description
- Impact
- Priority / Urgency
- Categorization
- Analysis Notes and Comments
- Cause / Determination
- Outcome / Resolution
- Lessons Learned

If a more detailed post-mortem is applicable, the Security and/or DevOps team will create the write-up and link it in the incident record.

Breach Investigation and Notification

2024.02.13

To provide guidance for breach notification when impressive or unauthorized access, acquisition, use and/or disclosure of the ePHI occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities and business associates may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

In the case of a breach, VigiLife shall notify all affected Customers. It is the responsibility of the Customers to notify affected individuals.

Policy Statements

VigiLife policy requires that:

(a) Breach notification procedures are invoked upon confirmation of security breach that results in unauthorized disclosure of unprotected/unencrypted sensitive data.

(b) Individuals impacted by a confirmed data breach must be notified within a predefined, required timeframe of discovery of such breach.

(c) In the event of a data breach that involves unencrypted ePHI, VigiLife must report the breach to individuals impacted following the HIPAA Breach Notification requirements (45 CFR Part 164, Subpart D).

Controls & Procedures

Breach Investigation Process

1. Discovery of Breach: A data breach shall be treated as "discovered" as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to VigiLife (includes breaches by the organization's Customers, Partners, or subcontractors). VigiLife shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or Partner of the organization. Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response) immediately, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each Customer affected by the

   breach. VigiLife shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: The VigiLife Security Officer shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of seven years. A breach log is kept and maintained by the Security and Privacy Officer.

3. Risk Assessment: A risk assessment is performed in accordance to applicable laws and regulations.

   For an acquisition, access, use or disclosure of ePHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. A use or disclosure of ePHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of ePHI constitutes a breach and requires further notification, the organization will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications to appropriate Customers or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

   - Consideration of who impermissibly used or to whom the information was impermissibly disclosed;
   - The type and amount of ePHI involved;
   - The cause of the breach, and the entity responsible for the breach, either Customer, VigiLife, or Partner.
   - The potential for significant risk of financial, reputational, or other harm.

4. Timeliness of Notification: Upon discovery of a breach, notice shall be made to the affected VigiLife Customers, usually within 24-48 hours but no later than 10 calendar days after the discovery of the breach. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

   - If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
   - If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:

   - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
   - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known;
   - Any steps the Customer should take to protect Customer data from potential harm resulting from the breach.
   - A brief description of what VigiLife is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
   - Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, a web site, or postal address.

7. Methods of Notification: VigiLife Customers will be notified via email and phone within the timeframe for reporting breaches, as outlined above.

8. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, VigiLife shall maintain a process to record or log all breaches of unsecured sensitive data regardless of the number of records and Customers affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):

   - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
   - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
   - A description of the action taken with regard to notification of patients regarding the breach.
   - Resolution steps taken to mitigate the breach and prevent future occurrences.

9. Workforce Training: VigiLife shall train all members of its workforce on the policies and procedures with respect to sensitive data as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

10. Complaints: VigiLife must provide a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures.

11. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforce, Customers, and Partners who fail to comply with privacy policies and procedures.

12. Retaliation/Waiver: VigiLife may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

VigiLife Platform Customer Responsibilities

The following requirements and guidelines shall be provided to and agreed upon by a client organization using VigiLife platform to host sensitive data such as ePHI and PII.

The agreement may be in the form of a contract or acceptance of terms and conditions.

1. The VigiLife Customer that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured sensitive data shall, without unreasonable delay and in no case later than 72 hours after discovery of a breach, notify VigiLife of such breach. The Customer shall provide VigiLife with the following information:
    - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
    - A description of the action taken with regard to notification of patients regarding the breach.
    - Resolution steps taken to mitigate the breach and prevent future occurrences.
2. Depending on the nature of the breach, an investigation may be conducted by VigiLife or the Customer or jointly to determine the cause of breach.
3. Notice to Media: Unless VigiLife is directly at fault for the cause of breach, VigiLife Customers are responsible for providing notice to prominent media outlets at the Customer's discretion.
4. Notice to Authorities: Unless VigiLife is directly at fault for the cause of breach, VigiLife Customers are responsible for providing notice to the appropriate authorities, including the Secretary of Health and Human Services (HHS) and your Lead Supervisory Authority (LSA) under GDPR, at the Customer's discretion.

Sample Letter to Customers in Case of Breach

[Date]

[Name] [Name of Customer] [Address 1] [Address 2] [City, State Zip Code]

Dear [Name of Customer] :

I am writing to you from VigiLife, Inc., with important information about a recent breach that affects your account with us. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known.
- Any steps the Customer should take to protect themselves from potential harm resulting from the breach.
- A brief description of what VigiLife is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

Other Optional Considerations:

- Recommendations to assist customer in remedying the breach.

We will assist you in remedying the situation.

Sincerely,

Robert Ficcaglia
Security Officer
VigiLife, Inc.
robert@sunstonesecure.com

List of Contacts for Authorities

Health and Human Services

- Phone: 1-877-696-6775
- Mailing Address: Centralized Case Management Operations U.S. Department of Health and Human Services 200 Independence Avenue, S.W. Room 509F HHH Bldg. Washington, D.C. 20201
- Website:

Federal Trade Commission

- Phone: 1-877-382-4357

- Website:

Indianapolis Metropolitan Police Department

- Phone: 317-327-3282
- Address: 50 N. Alabama St. Indianapolis, IN 46204

Federal Bureau of Investigation Indianapolis Office

- Phone: 317-595-4000
- Address: 8825 Nelson B Klein Pkwy Indianapolis, IN 46250

Third Party Security, Vendor Risk Management and Systems/Services Acquisition

2024.02.13

VigiLife makes every effort to assure all third party organizations are compliant and do not compromise the integrity, security, and privacy of VigiLife or VigiLife Customer data. Third Parties include Vendors, Customers, Partners, Subcontractors, and Contracted Developers.

Policy Statements

VigiLife policy requires that:

(a) A list of approved vendors/partners must be maintained and reviewed annually.

(b) Approval from management, procurement and security must be in place prior to onboarding any new vendor or contractor. Additionally, all changes to existing contract agreements must be reviewed and approved prior to implementation.

(c) For any technology solution that needs to be integrated with VigiLife production environment or operations, a Vendor Technology Review must be performed by the security team to understand and approve the risk. Periodic compliance assessment and SLA review may be required.

(d) VigiLife Customers or Partners should not be allowed access outside of their own environment, meaning they cannot access, modify, or delete any data belonging to other 3rd parties.

(e) Additional vendor agreements are obtained as required by applicable regulatory compliance requirements.

- A standard HIPAA Business Associate Agreement (BAA) is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements. A BAA must be signed with any vendor that may have a business need to access, and/or unsupervised access to PHI or ePHI.

Controls & Procedures

Vendor Technology Risk Review

VigiLife security policy requires a risk review of vendor technology, prior to any technology being integrated to VigiLife operations and/or infrastructure. Employees are required to engage security team to conduct such review. The request may be submitted by email directly to the security team, or by opening a GitHub Issues ticket through the VigiLife internal service desk.

Security team is responsible to conduct the reviews via interviews and reviews of documentation, to ensure the vendor complies with regulatory requirements and follows security best practices to minimize risk to an acceptable level.

A vendor technology risk (VTR) assessment is conducted using , in the following steps:

1. Reviewer sends questionnaire link(s) to vendor contact.
2. Vendor completes the questionnaire(s).
3. Vendor saves/exports answers to the assessment questionnaire(s).
4. Vendor contact sends the answers file back to reviewer.
5. Reviewer opens the same questionnaire(s) and loads the answers received from the vendor to complete the assessment.
6. Reviewer follows up with vendor contact as needed.
7. Reviewer facilities discussion with business owner to determine if the risk is acceptable. Vendor remediation may be required depending on the results.

A list of [approved vendors / contractors][1] is maintained by the Security and Operations teams. [1] :/approved-vendors/

Vendor Contractual Agreements

Vendor Contractual Agreements

HIPAA. If the vendor needs access to PHI/ePHI, the vendor must be HIPAA compliant and a [Business Associate Agreement (BAA)][BAA] is required. [BAA] :/hipaa-baa/

SLA for Service Providers. For network and infrastructure service providers that support production and/or critical operations at VigiLife, a Service Level Agreement (SLA) is defined and included in the service contract.

As appropriate, the executed agreement(s) are linked or attached to the vendor on the [approved vendors list][1]. [1] :/approved-vendors/

Monitoring Vendor Risks

Vendor contracts are reviewed either annually or according to the signed contract duration.

Based on the risk level and the sensitivity/criticality of data the vendor has access to, the vendor review may include an updated risk analysis performed by the security team in addition to legal and business review of contract terms.

If the vendor is a service provider, the DevOps team monitors the service status of the provider according to its SLA. This is done by either manually reviewing the posted service status on the vendor's status pages at least quarterly, or by setting up alarms for service interruption using automation.

Software and Systems Acquisition Process

VigiLife Security maintains a list of [pre-approved business software][1] and a list of [approved vendors / contractors][2]. [1] :/approved-software/ [2] :/approved-vendors/

If additional commercial software, hardware system, or cloud services is needed, a request should be submitted through VigiLife internal service desk. This will trigger the approval by manager/security and procurement process.

As applicable, VigiLife security team may conduct a risk analysis on the software or system to ensure it complies with VigiLife security, compliance and legal requirements and does not interfere with the security controls. If a risk is identified, additional controls should be identified and implemented (or planned) prior to acquisition. An alternative product may be considered as a result of the risk analysis.

Privacy and Consent

2024.02.13

VigiLife is committed to protecting the privacy of our customers.

Policy Statements

VigiLife policy requires that:

(a) Privacy policy shall be made available to inform Customers how VigiLife collects, uses, secures and shares customer information.

(b) Valid consent must be obtained for data collected from a Customer and the purposes data is used for must be provided. Customer must be provided an option to opt-in or opt-out.

Controls & Procedures

Privacy Policy

Current Privacy Policy is published at https://www.vigilife.com/privacy

Notice of Privacy Practice

Current Notice of Privacy Practice (NPP) is published at https://www.vigilife.com/privacy

Platform Use Terms and Consent

The Terms of Use and Consent for VigiLife platform and applications are hosted online or within the application itself.

Addendum and References

The following is a list of policy addendum and references.

References

Key Definitions

2024.02.13

- *Application*: An application hosted by VigiLife, either maintained and created by VigiLife, or maintained and created by a Customer or Partner.
- *Application Level*: Controls and security associated with an Application. In the case of PaaS Customers, VigiLife does not have access to and cannot assure compliance with security standards and policies at the Application Level.
- *Audit*: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing.
- *Audit Controls*: Technical mechanisms that track and record computer/system activities.
- *Audit Logs*: Encrypted records of activity maintained by the system which provide: 1) date and time of activity; 2) origin of activity (app); 3) identification of user doing activity; and 4) data accessed as part of activity.
- *Access*: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.
- *BaaS*: Backend-as-a-Service. A set of APIs, and associated SDKs, for rapid mobile and web application development. APIs offer the ability to create users, do authentication, store data, and store files.
- *Backup*: The process of making an electronic copy of data stored in a computer system. This can either be complete, meaning all data and programs, or incremental, including just the data that changed from the previous backup.
- *Backup Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all VigiLife Add-ons and as an option for PaaS Customers.
- *Breach*: A data breach is the intentional or unintentional release of secure or sensitive information to an untrusted environment or individual. A data breach often involves an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

  Under HIPAA, a data breach means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. Breach excludes:

  1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
  2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
  3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- *Business Associate*: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
- *Covered Entity*: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.
- *De-identification*: The process of removing identifiable information so that data is rendered to not be personally identifiable (not PHI).
- *Disaster Recovery*: The ability to recover a system and data after being made unavailable.
- *Disaster Recovery Service*: A disaster recovery service for disaster recovery in the case of system unavailability. This includes both the technical and the non-technical (process) required to effectively stand up an application after an outage. Offered with all VigiLife Add-ons and as an option for PaaS Customers.
- *Disclosure*: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
- *Customers*: Contractually bound users of VigiLife Platform and/or services.
- *Electronic Protected Health Information (ePHI)*: Any individually identifiable health information protected by HIPAA that is transmitted by, processed in some way, or stored in electronic media.
- *Environment*: The overall technical environment, including all servers, network devices, and applications.
- *Event*: An event is defined as an occurrence that does not constitute a serious adverse effect on VigiLife, its operations, or its

Customers, though it may be less than optimal. Examples of events include, but are not limited to:

  - A hard drive malfunction that requires replacement;
  - Systems become unavailable due to power outage that is non-hostile in nature, with redundancy to assure ongoing availability of data;
  - Accidental lockout of an account due to incorrectly entering a password multiple times.

- *Hardware (or hard drive)*: Any computing device able to create and store sensitive data (i.e. ePHI).
- *Health and Human Services (HHS)*: The government body that maintains HIPAA.
- *IaaS*: Infrastructure-as-a-Service.
- *Individually Identifiable Health Information*: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- *Indication*: A sign that an Incident may have occurred or may be occurring at the present time. Examples of indications include:

  - The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS "hits" are also false positives and are neither an event nor an incident;
  - The antivirus software alerts when it detects that a host is infected with a worm;
  - Users complain of slow access to hosts on the Internet;
  - The system administrator sees a filename with unusual characteristics;
  - Automated alerts of activity from log monitors like OSSEC;
  - An alert from OSSEC about file system integrity issues.

- *Intrusion Detection System (IDS)*: A software tool use to automatically detect and notify in the event of possible unauthorized network and/or system access.
- *IDS Service*: An Intrusion Detection Service for providing IDS notification to customers in the case of suspicious activity. Offered with all VigiLife Add-ons and as an option for PaaS Customers.
- *Law Enforcement Official*: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- *Logging Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all VigiLife Add-ons and as an option for PaaS Customers.
- *Messaging*: API-based services to deliver and receive SMS messages.
- *Minimum Necessary Information*: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "minimum necessary" standard applies to all protected health information in any form.
- *Off-Site*: For the purpose of storage of Backup media, off-site is defined as any location separate from the building in which the backup was created. It must be physically separate from the creating site.
- *Organization*: For the purposes of this policy, the term "organization" shall mean VigiLife.
- *PaaS*: Platform-as-a-Service.
- *Partner*: Contractual bound 3rd party vendor with integration with the VigiLife Platform. May offer Add-on services.
- *PMP or Platform*: VigiLife Precision Medicine Platform and its overall technical environment.
- *Protected Health Information (PHI)*: Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

  - Past, present or future physical or mental health or condition of an individual.
  - The provision of health care to an individual.
  - The past, present, or future payment for the provision of health care to an individual.

- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Sanitization*: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.
- *Trigger Event*: Activities that may be indicative of a security breach that require further investigation (See Appendix).
- *Restricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored, utilized, or accessible at any time.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Precursor*: A sign that an Incident may occur in the future. Examples of precursors include:

- Suspicious network and host-based IDS events/attacks;
- Alerts as a result of detecting malicious code at the network and host levels;
- Alerts from file integrity checking software;
- Audit log alerts.

- *Risk*: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of sensitive data, other confidential or proprietary electronic information, and other system assets.

- *Risk Management Team*: Individuals who are knowledgeable about the Organization's Privacy, Security and Compliance policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below.

- *Risk Assessment*:

  Referred to as Risk Analysis in the HIPAA Security Rule

  - Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
  - Prioritizes risks; and
  - Results in recommended possible actions/controls that could reduce or offset the determined risk.

- *Risk Management*: Within this policy, it refers to two major process components: risk assessment and risk mitigation.

  This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

- *Risk Mitigation*:

  Referred to as Risk Management in the HIPAA Security Rule

  A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

- *SaaS*: Software-as-a-Service.

- *Security Incident* (or just Incident): A security incident is an occurrence that exercises a significant adverse effect on people, process, technology, or data. Security incidents include, but are not limited to:

  - A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious;
  - Unauthorized disclosure;
  - Unauthorized change or destruction of sensitive data (i.e. deletion or alterations not following VigiLife's procedures);
  - Denial of service not attributable to identifiable physical, environmental, human or technology causes;
  - Disaster or enacted threat to business continuity;
  - Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:
  - Denial of Service: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources;
  - Malicious Code: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host;
  - Unauthorized Access/System Hijacking: A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations;
  - Inappropriate Usage: A person violates acceptable computing use policies;
  - Other examples of observable information security incidents may include, but are not limited to:
    - Use of another person's individual password and/or account to login to a system;
    - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment);
    - Installation of unauthorized software;
    - Terminated workforce member accessing applications, systems, or network.

- *Threat*: The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

  - Environmental - external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
  - Human - hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
  - Natural - fires, floods, electrical storms, tornados, etc.
  - Technological - server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
  - Other - explosions, medical emergencies, misuse or resources, etc.

- *Threat Source*: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect sensitive data.

- *Threat Action*: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

- *Unrestricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized or is not accessible there on a regular basis.

- *Unsecured Protected Health Information*: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

  1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such

into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
2. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
3. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPSec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
4. The media on which the PHI is stored or recorded has been destroyed in the following ways:
5. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
6. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

- *Vendor*: External individuals or organizations marketing or selling products or services, or providing services to VigiLife.
- *Vulnerability*: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.
- *Workstation*: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit sensitive data. Workstation devices may include, but are not limited to: laptop or desktop computers, smart phones, tablet PCs, and other handheld devices. For the purposes of this policy, "workstation" also includes the combination of hardware, operating system, application software, and network connection.
- *Workforce*: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Employee Handbook and Policy Quick Reference

2024.02.13

This is an abridged version of VigiLife's security policy that all workforce members are required to be familiar with and comply with.

You are assumed to have read and fully understood the corporate security and privacy policies, standards, guidelines, controls and procedures even if you haven't. So, it's probably best you still go through the whole thing at some point.

- First and foremost, as a Health IT provider, VigiLife and all its employees must fully comply with HIPAA Security and Privacy regulations. All workforce members much complete the required HIPAA training.
- You are required to follow detailed procedures defined in certain policies related to your job role.

Security is everyone's responsibility. If this is not your first job, don't do anything that might get you in trouble at your previous workplace. When in doubt, stop and ask.

Acknowledgement

As a VigiLife employee, I acknowledge that

* I have reviewed and will comply with company
  [security policies and procedures][1], [acceptable use][2], and [sanction policies][3].
* I accept that my work devices, including approved BYOD devices, and activities on such devices are subject to security monitoring.
* I will protect my work devices at remote locations and will not leave devices unattended.
* I will ensure my laptops and workstations are securely configured with whole disk encryption, endpoint security agent, malware protection, local firewall, password protected screensaver, and
* I will follow documented policies and procedures to protect sensitive and confidential data.
* I have completed the required [HIPAA awareness training][4].
* I understand that customer data and sensitive data may only be stored in approved production environments.
* I understand company and regulatory requirements to protect critical data and will NOT

  * store critical data such as customer data and passwords on online file shares (such as Google Drive, SharePoint, Dropbox), in logs and source codes;
  * send critical data such as customer data and passwords by email, chat, or similar public communication channels;
  * post critical data such as customer data and passwords in blogs, support tickets or other public forums; and
  * discuss patient information in public.

* I understand that use of paper records and fax transmission for sensitive customer data is not allowed.
* I will keep my passwords confidential and will NOT share my individual user passwords with other users.
* I will NOT use shared/generic, guest/anonymous, emergency or temporary accounts without explicit approval.
* I will regularly back up business data on my user devices to approved data storage media/repositories such as the company SharePoint site.
* I will report any incident and suspicious activity to Security and/or my manager.

[1] : https://www.vigilife.com/security [2] : #acceptable-use-policy-for-end-user-computing [3] :/hr/non-compliance-investigation-and-sanctions [4] :

Training

You will be prompted as part of onboarding, and periodically going forward, to complete the following security training:

- **General security policy and procedures** training, including
    - Roles, Responsibilities and Training
    - HR and Personnel Security
    - Data Classification and Handling
- **HIPAA awareness** training
- **Ongoing security awareness** training (a monthly series, currently provided by)
- **Role-based security** training
    - all members of the **Development/Engineering** team must carefully review the following policies and procedures
        - Product Security and Secure Software Development
        - HIPAA Best Practices for Software Development
        - Data Management
        - Data Protection
        - Configuration and Change Management
    - all members of the **Administrative**, **Marketing** and **Procurement** teams must review the following policies and procedures
        - Third Party Security, Vendor Risk Management and Systems/Services Acquisition
    - all members of the **Administrative** and **Senior Leadership/Executive** teams must review the following policies and procedures
        - Business Continuity and Disaster Recovery
        - Compliance Audits and External Communications
        - Risk Management
    - all members of the **HR** and **Facilities** teams must review the following policies and procedures
        - HR and Personnel Security
        - Facility Access and Physical Security
    - all team members responsible for **Product Management** and **Business Development** must review the following policies and procedures
        - Privacy and Consent
    - all members of the **Security**, **Compliance** and **IT** teams must review all policies and procedures in its entirety

Acceptable use policy for end-user computing

VigiLife policy requires that:

(a) Per VigiLife security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of VigiLife computing systems is subject to monitoring by VigiLife IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that are commonly affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the VigiLife Data Classification specifications and Data Handling procedures.

(j) Mobile devices are not allowed to connect directly to VigiLife production environments.

(k) It is strictly forbidden to download or store any ePHI on end-user computing devices, including laptops, workstations and mobile devices.

Your responsibilities for computing devices

VigiLife provides company-issued laptops and workstations to all employees. VigiLife currently does not require or support employees bringing their own computing devices.

The laptops and/or workstations assigned to you are yours to configure and manage according to company security policy and standards. You are responsible to

- configure the system to meeting the configuration and management requirements, including password policy, screen protection timeout, host firewall, etc.;
- ensure the required anti-malware protection and security monitoring agent is installed and running; and
- install the latest security patches timely or enable auto-update.

IT and Security provides automated scripts for end-user system configurations and/or technical assistance as needed.

You are also responsible for maintaining a backup copy of the business files local on your laptop/workstation to the appropriate location on VigiLife file sharing / team site (e.g. SharePoint). Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams
- Meeting notes/recordings
- Important records (e.g. approval notes)

Important

DO NOT backup critical data such as customer data or PII to file sharing sites.
If you have such critical data locally on your device, contact IT and
Security for the appropriate data management and protection solution.

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet VigiLife requirements).

Getting help

Support for most of our business applications are self-service, such as password reset via Okta.

If needed, users may use our internal service desk to request IT and Security support. Common requests include:

- Password reset and access requests
- Request new software and hardware
- Technical support
- Recommend changes to policies and processes

How to report an incident or suspicious activity

You are responsible to report all suspicious activities and security-related incidents immediately to the Information Security team, by one of the following channels:

- (preferred) “Report a security incident” by creating an issue on GitHub Issues and/or via the [internal help desk]() (mailto:security@vigilife.com)
- For non-sensitive, non-confidential security issues and concerns, employees may post questions on VigiLife’s #infosec Slack channel.
- Additionally, employees may report the incident to their direct manager.
- To report a concern under the Whistleblower Policy, you may first discuss the concerns with your immediate manager, or report it directly to the CEO or COO. *See the [Whistleblower Policy section in the HR Security Policy][5] for additional details.* [5] :/hr/whistleblower-policy

Approved Software

2024.02.13

Software approved for use at VigiLife includes, but is not limited to:

- Adobe suite
- Atlassian suite

- Code editors (Atom, Emacs, Vim, VS Code, etc)
- Dashlane
- Docker
- Node/NPM
- Office 365
- Okta (and any apps/services managed by Okta)
- Postman
- Slack
- Sketch
- Zoom

Reputable and well documented open source / free software may be used for development purposes at the discretion of the Engineering team. Cb Defense agents must be active to monitor the behavior of all application processes. Additional periodic audit may be conducted to review the usage of open source tools. Examples of such software include, but are not limited to:

- Chrome and various browser extensions
- Firefox and various browser extensions
- Homebrew
- GraphQL/GraphiQL
- Keybase
- Skitch
- Spectacle
- etc.

Software not in the list above may be installed if it is necessary for a business purpose, legal, with a valid license, and approved on a case-by-case basis by your manager or the Security Officer.

Approved Vendors

2024.02.13

For confidentiality reasons, the list of approved vendors is maintained internally at company Wiki / SharePoint site.

Cookie Policy

Updated:

We at VigiLife (VigiLife, Inc. and our subsidiaries and affiliates) are committed to protecting your privacy. We and our partners use cookies and similar technologies on our services, including our websites and mobile applications (the "Services"). This Cookie Policy explains these technologies, why we use them, and the choices you have.

By visiting or using our Services, you are consenting to us gathering and processing information (as defined in our Privacy Policy) about you in accordance with this Cookie Policy.

TECHNOLOGIES WE USE

Like many Internet-enabled services, we use technologies that place small files/code on your device or browser for the purposes identified in our Privacy Policy, primarily to remember things about you so that we can provide you with a better experience.

Cookies. A cookie is a small data file stored on your browser or device. They may be served by the entity that operates the website you are visiting ("first-party cookies") or by other companies ("third-party cookies").

- For example, we partner with third-party analytics providers, like Google, which set cookies when you visit our websites. This helps us understand how you are using our Services so that we can improve them.

Pixels (Clear Gifs/Web Beacons/Web Bugs/Embedded Pixels). These are small images on a web page or in an email. They collect information about your browser or device and can set cookies.

Local Storage. Local storage allows data to be stored locally on your browser or device and includes HTML5 local storage and browser cache.

Software development kits (“SDKs”). SDKs are blocks of code provided by our partners that may be installed in our mobile applications. SDKs help us understand how you interact with our mobile applications and collect certain information about the device and network you use to access the application.

OUR USE OF THESE TECHNOLOGIES

Below are the ways that we and our partners use these technologies on our Services.

CATEGORY OF USE	PURPOSE OF USE

CATEGORY OF USE	PURPOSE OF USE
Preferences	To help us remember your settings and preferences so that we can provide you with a more personalized experience.
Authentication and Security	To log you into the Services; enable us to show you your account data; and help us keep your data and the Services safe and secure.
Service Features and Performance	To provide you with functionality and optimize the performance of the Services. For example, to allow you to share information from VigiLife mobile apps with friends within your social networks/circles.
Analytics and Research	To help us understand how you are using the Services so that we can make them better, faster, and safer.

YOUR CHOICES

You have a number of options to control or limit how we and our partners use cookies and similar technologies, including for advertising. Please note that VigiLife websites and our Services do not respond to Do Not Track signals because we do not track our users over time and across third-party websites to provide targeted advertising. However, we believe that you should have a choice regarding interest-based ads served by our partners, which is why we outline the options available to you here below.

You can set your device or browser to accept or reject most cookies, or to notify you in most situations that a cookie is offered so that you can decide whether to accept it. However, if you block cookies, certain features on our Services may not function. Additionally, even if you block or delete Cookies, not all tracking will necessarily stop.

- To prevent your data from being used by Google Analytics, you can install Google's opt-out browser add-on.
- For information on how our advertising partners allow you to opt out of receiving ads based on your web browsing history, please visit .
- To opt out of ads on Facebook, Pinterest, Google or other sites that are targeted to your interests, use your Facebook, Pinterest, Google Ads, or the other site settings.
- Check your mobile device for settings that control ads based on your interactions with the applications on your device. For example, on your iOS device, enable the "Limit Ad Tracking" setting, and on your Android device, enable the "Opt out of Ads Personalization" setting.

As an additional step, these advertising companies may participate in one of the following advertising industry self-regulatory programs for online behavioral advertising, with corresponding user opt-outs:

- Networking Advertising Initiative () (US Only)
- Digital Advertising Alliance () (US Only)
- European Interactive Digital Advertising Alliance () (EU Only)
- Digital Advertising Alliance - Canada () (Canada Only)
- DAA App Choices Mobile App (Mobile Devices Only) - For mobile devices (e.g., smartphone, tablets), you may consider downloading the DAA AppChoices Mobile App to manage such technology.

CONTACT US

If you have questions about our use of cookies and similar technologies, please contact us at privacy@vigilife.com.

Privacy Officer
VigiLife, Inc.

Privacy Policy

Updated:

We at VigiLife (VigiLife, Inc. and our subsidiaries and affiliates) are committed to protecting your privacy. This privacy policy applies to our applications, software, websites, APIs, products, and services including our associated mobile applications ("Mobile Apps"), (each a "Site",

"Service", or "Mobile App" or collectively, the "Services"), owned and controlled by VigiLife.

This Privacy Policy governs our data collection, processing and usage practices. It also describes your choices regarding use, access and correction of your personal information. If you do not agree with the data practices described in this Privacy Policy, you should not use our Services.

Specifically, this Privacy Policy covers:

Topic	Summary

Topic	Summary
Information we collect about you	We may collect Personal Information, Usage and Device Information (collectively, "information", defined in detail below) about you in connection with your (or your organization's) use of our Services that link to this Privacy Policy. Learn more below
How we use your information	We use the information we collect only in compliance with this Privacy Policy. We may use your information to provide services (either directly to you or to those third parties who have engaged us as service providers to process your information on their behalf); respond to inquiries and provide customer support and technical assistance; communicate with you; process transactions; improve, develop, provide content for, operate, deliver and market our Services; implement social networking features; comply with our company policies and procedures and with applicable law; ensure proper and authorized use of the Services; perform Services tracking and analysis; and, as otherwise permitted by applicable law. Learn more below
How we share your information	We may share your information with our business units, affiliates, subsidiaries, business partners, service providers and/or your representatives, in order to provide or improve our Services to you. We do not share information with third parties so that they can independently market their own products or services to you unless we have explicitly given you the option to opt-in such disclosures. We will never sell your Personal Information to any third party. Learn more below
Your Rights Regarding Your Personal Information	We provide you with the opportunity to be informed of whether we are processing your information and to access, correct, update, oppose, delete, block, limit or object, upon request and free of charge, to our use of your Personal Information to the extent required by applicable law. Learn more below
Retention of your information	We keep your account information, like your name, email address, and password, for as long as your account is in existence because we need it to operate your account. In some cases, when you give us information for a feature of the Services, we delete the data after it is no longer needed for the feature. We keep your account data until you use your account settings or tools to delete the data or your account because we use this data to provide you Services. We also keep information about you and your use of the Services for as long as necessary for our legitimate business interests, for legal reasons, and to prevent harm, including as described in the How We Use Your Information and How We Share Your Information sections.
Security of your information	We work hard to keep your data safe. We use a combination of technical, administrative, and physical controls to protect the confidentiality, integrity and availability of your data. This includes using Transport Layer Security ("TLS") to encrypt data transmission and Advanced Encryption Standard ("AES") to encrypt data storage. No method of transmitting or storing data is completely secure, however. If you have a security-related concern, please contact Customer Support or our Security team. Click here to learn more about our security practices.
International	VigiLife is a U.S.-based company that offers our Services to U.S. and international customers. As a result, information that we collect, including personal information, may be transferred to our data centers or service providers in the U.S. By providing your personal information to us, you are consenting to the transfer of your personal information to the U.S. and to our (and our services providers') use and disclosure of your personal information in accordance with this Privacy Policy. We rely on multiple legal bases to lawfully transfer personal data around the world. These include your consent, the EU-US and Swiss-US Privacy Shield. VigiLife complies with the Privacy Shield principles regarding the

Topic	Summary
International Data Transfers	the EU-US and Swiss-US Privacy Shield. VigiLife complies with the Privacy Shield principles regarding the collection, use, sharing, and retention of personal information as described in our Privacy Shield certifications, and we follow internal procedures for verifying that our commitments under this Privacy Policy have been implemented. Our compliance with this obligation can be investigated and enforced by the U.S. Federal Trade Commission. Learn more about Privacy Shield here. If you have a complaint about our Privacy Shield compliance, please contact us. You can also refer a complaint to our chosen independent dispute resolution body JAMS, and in certain circumstances, invoke the Privacy Shield arbitration process or lodge a complaint with the supervisory authority in your country of residence in the EU.
Cookies and similar Technologies	We may use “cookies” and similar technologies to help deliver our Services. This technology may involve placing small files/code on your device or browser that serve a number of purposes, such as remembering your preferences and to offer you a more personalized user experience. Read our Cookie Policy to learn more.
Marketing Analytics and Communications	We work with partners who provide us with marketing analytics and communications services. This includes helping us understand how users interact with our Services, communicating with you about our Services and features, and measuring the performance of those communications. These companies may use cookies and similar technologies to collect information about your interactions with the Services and other websites and applications. To learn more and about your privacy choices, please see more details in the How We Use Your Information and How We Share Your Information sections and read our Cookie Policy.
Links to Other Websites	Our Services may contain links to other websites or services that are not owned or controlled by VigiLife, including links to websites of our sponsors and partners. This Privacy Policy only applies to information collected by our Services. We have no control over these third-party websites, and your use of third party websites and features are subject to privacy policies posted on those websites. We are not responsible or liable for the privacy or business practices of any third-party websites linked to our Services. Your use of third parties’ websites linked to our Services is at your own risk, so we encourage you to read the privacy policies of any linked third-party websites when you leave one of our Services.
Our Policies for Children	Our Services are directed toward adults. If you are under the age of 16, you must obtain the authorization of a responsible adult (parent or legal custodian) before using or accessing our Services. We will not knowingly collect or use any personal information from any children under the age of 16. If we become aware that we have collected any personal information from children under 16, we will promptly remove such information from our systems.
Situations where this Privacy Policy does not apply	This Privacy Policy does not apply to job applicants or employees, which are subject to relevant privacy notices. This Privacy Policy does not apply to the extent that: • Our products and services set forth an additional or alternative Privacy Policy; or • Applicable law imposes different processing or privacy requirements on your information.
Changes to this Privacy Policy	We periodically update this Privacy Policy. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice by sending you notification by email or notification alert within our Services. While we will notify you of any material changes to this Privacy Policy, we encourage you to review this Privacy Policy periodically. We will also keep prior versions of this Privacy Policy in an archive for your review.
How to contact us	You can contact us using the Contact Us page on our Sites or by mail at . If you have questions, suggestions, or concerns about this policy, or about our use of your information, including filing a complaint, please contact our Data Protection Officer or Privacy Officer at privacy@vigilife.com.

INFORMATION WE COLLECT ABOUT YOU

When you use our Services, we collect the following types of information.

INFORMATION YOU PROVIDE US ("PERSONAL INFORMATION")

ACCOUNT INFORMATION. Some information is required to create an account on Services, such as your

- name,
- email address,
- password,
- company, and
- phone number.

ADDITIONAL INFORMATION. To help improve your experience or enable certain features of the Services, you may choose to provide us with additional information, such as

- a profile photo,
- biography,
- mailing address,
- country information,

- date of birth,
- gender,
- height,
- weight,
- additional health information or activity data such as your logs for food, weight, sleep, water,
- additional contact phone numbers such as your mobile telephone number,
- community or social media username, and
- messages on discussion boards or to your social contacts on the Services.

You may also connect with friends on the Services or invite friends who have not yet joined by providing their email addresses, accessing social networking accounts or using the contact list on your mobile device. We do not store your contact list and delete it after it is used for adding contacts as friends.

If you contact us or participate in a survey, contest, or promotion, we collect the information you submit such as your name, email address, contact information, and message.

INFORMATION FROM THIRD-PARTY SERVICES. If you choose to connect your account on our Services to your account on another service, we may receive information from the other service. For example, if you connect to Facebook or Google, we may receive information like your name, profile picture, age range, language, email address and friend list. You may also choose to grant us access to your personal information such as activity data or health data from other services. You can stop sharing the information from the other services with us by removing our access to each other service.

INFORMATION PROVIDED BY OTHER INDIVIDUALS. While using our Services, individuals may provide information about another individual, or an authorized user (such as an account administrator) creating an account on your behalf may provide information about You. When one individual provides us with information (including personal information) about another individual, we assume that the individual has permission and authority to do so and to consent on behalf of that individual to the collection and use of personal information as described in this Privacy Policy. Please contact us immediately if you become aware of an individual providing us with personal information about another individual without being authorized to do so, and we will act consistently with this Privacy Policy.

PAYMENT AND CARD INFORMATION. Some VigiLife Services support payments and transactions with third parties. If you activate this feature, you must provide certain information for identification and verification, such as your name, billing address, credit, debit or other card number, card expiration date and CVV code. This information is used solely to check your financial qualifications and collect payment from you. We do not store your payment information. We use a third-party service provider to manage payment card processing. Note that third-party payment processors may retain this information in accordance with their own privacy policies and terms. This service provider is not permitted to store, retain or use information you provide except for the sole purpose of credit card processing on our behalf.

INFORMATION WE RECEIVE FROM YOUR USE OF OUR SERVICES

USAGE AND DEVICE INFORMATION. When you use our Services, we receive certain usage data ("Usage and Device Information"). This includes information about your interaction with the Services, for example, when you view or search content, install or open applications or software, create or log into your account, import data into your account, or integrate a third-party service to your account. We may also collect data about the devices and computers you use to access our Services, including IP addresses, browser type, language, operating system, or mobile device information (including device and application identifiers), the referring web page, pages visited, location (depending on the permissions you have granted us), and cookie information.

HEALTH AND OTHER SPECIAL CATEGORIES OF PERSONAL DATA. To the extent that information we collect directly from you is health data or another special category of sensitive personal data subject to the European Union's General Data Protection Regulation ("GDPR"), we ask for your explicit consent to process such sensitive personal data. We obtain this consent separately when you take actions leading to our obtaining the data, for example, when you activate the activity tracking features in our Mobile Apps or grant us access to your health or activity data from another service. You can use your account settings or contact us to withdraw your consent at any time, including by stopping use of a feature, removing our access to a third-party service, requesting deletion your data or closing your account.

However, if we are acting as a service provider (a "Data Processor") processing your personal information on behalf of a third party that has collected such data from you, and such third party is the party that has the right to determine the purposes for which it will process your personal information and the means it will use to process your personal information (the "Data Controller"), then such Data Controller has the legal obligation to ask for your explicit consent to process your sensitive personal data (including health data), and we are not responsible for obtaining such consent from you. In such a scenario, the Data Controller may have their own, separate policies regarding the use and disclosure of your personal information, including any sensitive personal data you provide to such Data Controller. In such a scenario, this Privacy Policy does not apply to, we cannot control the activities of, and we are not responsible for the activities of the applicable Data Controller generally; this Privacy Policy only applies to our processing of your personal information that we, as a Data Processor, have been asked to process on behalf of the Data applicable Data Controller. We encourage you to review such Data Controller's privacy policy and/or contact the applicable Data Controller for more information about the policies that apply to their use and disclosure of your personal information, including any sensitive personal data.

HOW WE USE YOUR INFORMATION

We use the information we collect for the following purposes.

PROVIDE AND MAINTAIN THE SERVICES

We use the information we collect to deliver the Services to you and honor our Terms of Service for each Service or business contract with you. For example,

- to administer, operate, maintain and secure our Services;

- to monitor and analyze trends, usage and activities in connection with our Services;
- for accounting, recordkeeping, backup and administrative purposes;

- to customize and improve the content of our communications, websites and social media accounts;
- to provide customer service and support;
- to communicate with you, including responding to your comments, questions and requests regarding our Services;
- to process and complete transactions, and send you related information, including alerts and notifications about your service, purchase confirmations and invoices; and
- to educate and train our workforce in data protection and customer support.

For the Services' social features, we may use your information to help you find and connect with other users and to allow other users to find and connect with you. For example, your account contact information allows other users to add you as a friend. When another user has your email or mobile phone number in their contact list or in their friend network on a connected service, we may show that user that you are a user of the Services.

IMPROVE, PERSONALIZE, AND DEVELOP THE SERVICES

We use the information we collect to improve and personalize the Services and to develop new ones. For example, we use the information to troubleshoot and protect against errors; perform data analysis and testing; conduct research and surveys and develop new features and Services.

COMMUNICATE WITH YOU

We use your information when needed to send you Service notifications and respond to you when you contact us. We also use your information to promote new features or products that we think you would be interested in. You can control marketing communications and most Service notifications by using your notification preferences in account settings or via the "Unsubscribe" link in an email.

PROMOTE SAFETY AND SECURITY

We use the information we collect to promote the safety and security of the Services, our users and other parties. For example, we may use the information

- to authenticate users;
- to facilitate secure payments;
- to respond to a legal request or claim, conduct audits, and enforce our terms and policies;
- to investigate and protect against fraud, malicious or unauthorized access, and other illegal activities; and
- to demonstrate and verify compliance with our internal policies and procedures, and applicable privacy and data security laws and regulations, such as HIPAA and GDPR.

USE AND DISCLOSURE OF DE-IDENTIFIED INFORMATION

"De-identified" means that we have removed, or rendered unreadable through complex computational algorithms, your personally-identifiable information, such as your name, address, or birthdate. We may use de-identified information that we have obtained from our Services for various purposes, including for example:

- In accordance with regulatory requirements, we may de-identify, store and use your information for internal quality control, validation and research and development. This is important for VigiLife to maintain high quality Services. We may use de-identified information as permitted by law.
- We may contribute de-identified genetic variants that we have observed in the course of providing our Services to publicly available databases such as ClinVar. We do this to increase understanding and raise awareness of the significance of genetic variants within the medical and scientific communities.
- We may use or disclose de-identified information for general research and communications purposes. This may include analysis of this information to communicate observations and learnings, for example in the case of aggregated data. This may also include research collaborations with third parties, such as universities, hospitals or other laboratories, in which we utilize de-identified clinical cases, at the individual level or in the aggregate, in accordance with our study protocols, and we may present or publish such information. This may also include commercial collaborations with private companies for purposes such as to determine the prevalence of particular disorders or variants among the patients we have tested, or to determine whether any of the patients we have tested might be suitable for potential recruitment for research, clinical trials, or clinical care; however, we will not directly contact these patients about these opportunities without their prior written consent.

We use cookies and similar technologies for the purposes described above. For more information, please read our Cookie Policy.

For personal data subject to the GDPR, we rely on several legal bases to process the data. These include when you have given your consent, which you may withdraw at any time using your account settings and/or other tools; when the processing is necessary to perform a contract

with you, like the Terms of Service; and our legitimate business interests, such as in improving, personalizing, and developing the Services, marketing new features or products that may be of interest, and promoting safety and security as described above.

HOW WE SHARE YOUR INFORMATION

We do not share your personal information except in the limited circumstances described below.

WHEN YOU AGREE OR DIRECT US TO SHARE

You may direct us to disclose your information to others, such as when you use our social features in our Mobile Apps. For certain information, you may change your privacy preferences in account settings and use other provided tools to control how your information is visible to other users of the Services.

You may also authorize us to share your information with others, for example, with a third-party application when you give it access to your

account, or with your employer company or other organizations and provide consent to each organization. Remember that their use of your

information will be governed by their privacy policies and terms. You can revoke your consent to share with third-party applications or employee wellness programs using your account settings.

FOR EXTERNAL PROCESSING

We transfer information to our corporate affiliates, service providers and other partners who process it for us, based on our instructions and in compliance with this policy and any other appropriate confidentiality and security measures. These partners provide us with services globally, including for customer support, information technology, payments, sales, marketing, data analysis, research and surveys.

FOR LEGAL REASONS OR TO PREVENT HARM

We may preserve or disclose information about you to comply with a law, regulation, legal process or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect or investigate illegal activity, fraud, abuse, violations of our terms or threats to the security of the Services or the physical safety of any person. Please note: Our policy is to notify you of legal process seeking access to your information, such as search warrants, court orders or subpoenas, unless we are prohibited by law from doing so. In cases where a court order specifies a non-disclosure period, we provide delayed notice after the expiration of the non-disclosure period. Exceptions to our notice policy include exigent or counterproductive circumstances, for example, when there is an emergency involving a danger of death or serious physical injury to a person. We may share non-personal information that is aggregated or de-identified so that it cannot reasonably be used to identify an individual. We may disclose such information publicly and to third parties, for example, in public reports about exercise and activity, to partners under agreement with us or as part of the community benchmarking information we provide to users of our subscription services. If we are involved in a merger, acquisition, or sale of assets, we will continue to take measures to protect the confidentiality of personal information and give affected users notice for the transferring of any personal information to a new entity.

YOUR RIGHTS REGARDING YOUR PERSONAL INFORMATION

You can access and control your personal information via account settings and/or our tools we provide to you, regardless of where you live. If you live in the European Economic Area, United Kingdom and Switzerland (the “Designated Countries”), you have a number of legal rights with respect to your information, as outlined below.

Accessing and Exporting Data. By logging into your account, you can access much of your personal information. Using your account settings or by contacting us, you can also request a download information in a commonly used file format, including data about your activities, body, foods and sleep.

Editing and Deleting Data. Your account settings and certain platform APIs let you change and delete your personal information and/or account data. For instance, you can edit or delete the profile data you provide and delete your account if you wish.

If you choose to delete your account, please note that while most of your information will be deleted within 14 days, it may take up to 90 days to delete all of your information, such as the data stored in our backup systems. This is due to the size and complexity of the systems

we use to store data. We may also preserve data for legal reasons or to prevent harm, including as described in the How We Share Your Information section.

Objecting to Data Use. You can control usage of your data via account settings or other application APIs or tools. For example, you can

- limit how your information is visible to other users of the Services;
- limit the notifications you receive from us; and
- revoke the access of third-party applications that you previously connected to your account.

If you live in a Designated Country, in certain circumstances, you can object to our processing of your information based on our legitimate interests, including as described in the How We Use Information section. You have a general right to object to the use of your information for direct marketing purposes. Please also review our Cookie Policy for your options to control how we and our partners use cookies and similar technologies for advertising.

Restricting or Limiting Data Use. In addition to the various controls that we offer, if you reside in a Designated Country, you can seek to restrict our processing of your data in certain circumstances. Please note that you can always delete your account at any time.

Onward Transfers of Data. If we intend to disclose your personal information to any third party that will have the right to process it, we will enter into a contract with that third party that provides that your personal information may be processed only for limited and specified purposes consistent with the consent you have provided to us, and that the third party must provide the same level of protection for your personal information that we are obligated to provide under this Privacy Policy while it is processing your personal information. In addition, we will notify you if that third party will have the right to determine the purposes for which it will process your personal information and the means it will use to process your personal information (rather than just providing requested assistance to us in support of our permitted uses of your personal information).

Changes to Privacy Policy. If we are using your personal information on the basis of your consent, and we change our Privacy Policy to permit any use or disclosure of your personal information that is materially different than the uses for which it was originally collected or subsequently authorized by you, we will obtain your consent before we make such further uses of your personal information.

Further Assistance. If you need further assistance regarding your rights, please contact our Data Protection Officer at privacy@vigilife.com, and we will consider your request in accordance with applicable laws. If you reside in a Designated Country and you are not satisfied with our response, you will have a prompt, no-cost way of asserting your claim by contacting our chosen independent dispute resolution body JAMS. If you reside in a Designated Country, you may have the right, under certain conditions, to invoke binding arbitration, and, alternatively, you also have a right to lodge a complaint with your local data protection authority or with the Irish Data Protection Commissioner, our lead supervisory authority, whose contact information is available here.

VigiLife HIPAA Business Associate Agreement ("BAA")

2024.02.13

Introduction

This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. This sample is created by Office for Civil Rights (OCR), available online at the [HHS website][1].

[1] : https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide

the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in

which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of

disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

SIGNATURE FOLLOWS

GDPR Data Processing Agreement/Addendum ("DPA")

Data Protection Addendum

This Data Protection Addendum (this "Addendum") is made and entered into as of the date appearing on the signature page hereto (the "Effective Date") by and between VigiLife, Inc. ("Company") and the Supplier named on the signature page hereto, and upon execution shall be incorporated by reference into each agreement for services ("Services Agreement") pursuant to which Supplier may Process (as defined below) Personal Data (as defined below) for, from, or on behalf of Company.

A. Personal Data Protection

For the purposes of this Addendum, the terms "Controller", "Data Subjects", "Personal Data", "Personal Data Breach", "Processor" and "Process" shall have the meaning as defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") or any successor European Union data protection framework.

The parties agree that to the extent Supplier, in the context of performing the agreed services, processes any Personal Data of Company, Supplier shall be the Processor and Company shall be the Controller of such Personal Data. Notwithstanding any obligations of Company as Controller under applicable data protection law, Supplier undertakes the following as Processor:

(a) to process any Personal Data only on behalf and in accordance with Company's documented instructions and not for any purposes other than those described in this Addendum, unless (i) Company has given its express prior consent or (ii) Supplier is strictly required to do so under applicable European Data Protection Law (as defined below); in such a case, Supplier shall inform Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects are further specified in Exhibit 1 to this Addendum.

(b) to comply with (i) the GDPR and any applicable European data protection laws and regulations (collectively "European Data Protection Law"), and (ii), in case Supplier is certified under the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework, or any successor program recognized under European Data Protection Law to provide for an adequate level of data protection, the principles of such applicable Privacy Shield Framework or successor program, and (iii) all other applicable data protection and privacy laws and regulations ((i) to (iii) collectively "Data Protection Laws").

(c) to implement appropriate technical and organizational measures in such a manner that the Processing, including by any Sub-Processors (as defined below), will meet the requirements under Data Protection Laws and ensure the protection of the rights of the Data Subjects, and to regularly test, assess and evaluate the effectiveness of and, as necessary, improve and update these measures. The measures shall ensure a level of data security appropriate to the risks for the rights and freedoms of the Data Subjects. In particular, Supplier shall protect the personal data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

(d) to keep Personal Data strictly confidential and to ensure, and be able to demonstrate on request, that (i) only those persons have access to the Personal Data who are authorized by Supplier and have a strict need to know the data for the purposes under this Addendum, and (ii) all persons with access to Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(e) to disclose Personal Data to third parties, including affiliated companies, and/or to engage another Processor for the Processing of Personal Data ("Sub-Processor") only with Company's express prior consent. Where Supplier is authorized to engage another Sub-Processor for carrying out Processing activities on behalf of Company, Supplier shall enter into a written contract with the Sub-Processor which (i) imposes on the Sub-Processor the same data protection obligations as set forth in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements under Data Protection Laws, and (ii) grants Company the right to directly audit the Sub-Processor as set forth under Section A(j). Supplier shall promptly send a copy of any sub-processor agreement it concludes under this Section A(e) to Company. Supplier shall select the Sub-Processor diligently, taking into account the technical and organizational measures it has implemented, and ensure, by carrying out audits before and regularly after the commencement of the data processing by such Sub-Processor, that it maintains appropriate technical and organizational measures to safeguard an adequate level of data protection within the meaning of European Data Protection Law. Supplier shall remain fully liable to Company for the performance of this Agreement and be responsible and liable for any act or omission of the Sub-Processor with respect to its data protection obligations.

(f) to assist Company, including by appropriate technical and organizational measures, insofar as this is possible and taking into the nature of the processing, in fulfilling its obligations in relation to requests from Data Subjects for exercising their Data Subject's rights under Data Protection Laws, including, but not limited to, the Data Subject's right of access, right to rectification and erasure, right to restriction of processing, right to data portability and right to object, as provided for under the GDPR.

(g) to assist Company, taking into account the nature of the processing and information available to Supplier, in ensuring compliance with the obligations under applicable Data Protection Laws, including, in particular, by providing all information and assistance to enable Company (i) to comply with applicable data security obligations, (ii) to carry out a data protection impact assessment or prior consultation with the supervisory authority, as required under European Data Protection Law, and (iii) to respond promptly and properly to any enquiries concerning the Processing of Personal Data and cooperate in good faith with the supervisory authorities, the Data Subjects or any third party within a reasonable time. Supplier shall not communicate with any supervisory authority, Data Subject or any third party in connection with the Processing of Company's Personal Data without prior approval from Company, except as expressly permitted in this Section A.

(h) to notify Company, without undue delay, in writing or via e-mail (i) of any intended change of the locations currently set out in Exhibit 1 to this Addendum for the Processing of Personal Data, (ii) in case of a dispute, claim or request brought by a Data Subject directly against Supplier, (iii) in the event of any measure, request or other communication by a supervisory authority, including about any legally binding request for access or disclosure of Personal Data by a public authority (unless otherwise legally prohibited, in which case the Supplier will use its best efforts to obtain the right to waive this prohibition), and provide reasonable assistance if Company wishes to contest the request, and (iv) of any suspected or actual Personal Data Breach, any breach of applicable Data Protection Laws or of this Addendum. Supplier shall promptly remedy any breach and cooperate with Company in the investigation and remedy of such breaches and provide all reasonable assistance and information to enable Company to comply with, or, as applicable, to avoid, any data breach notification obligations vis-à-vis supervisory authorities and/or Data Subjects. Supplier shall further immediately inform Company if, in its opinion, an instruction infringes Data Protection Laws and/or Supplier becomes aware of the existence of any local laws that would have a substantial adverse effect on the guarantees and undertakings provided for under this Addendum.

(i) at the choice of Company, to return to Company (in a standard format facilitating portability) and/or to securely delete/destroy all Personal Data, including all existing copies thereof, in accordance with Company's instructions, within thirty (30) days upon Company's request or after the end of the provision of the services relating to Processing, and to certify to Company in writing that it has done so. Supplier shall not be obliged to delete/destroy all copies of the Personal Data where a longer storage by Supplier is required under European Data Protection Law, in which case Supplier shall inform Company accordingly, including about the legal grounds for, and the term of, any further storage;

(j) to make available to Company all information necessary to demonstrate compliance with the obligations under Data Protection Laws applicable to Company and to allow for and contribute to audits, including on-site inspections, conducted by Company or another auditor mandated by Company. (k) to enter into any further agreements that may be required under Data Protection Laws relating to Personal Data, and to provide all other assistance and support to Company.

B. Changes to this Addendum

The parties agree that, to the extent required under applicable Data Protection Laws, such as due to legislative changes, court decisions, and/or to reflect measures or guidance from the competent supervisory authorities or the European Commission, including, without limitation, the adoption of standards for contracts with processors according to Art. 28(7) or (8) GDPR or the invalidation, amendment, replacement or repeal of a decision adopted by the EU Commission in relation to international data transfers on the basis of Art. 45(3) or Art. 46(2) GDPR or on the basis of Article 25(6) or 26(4) of EU Directive 95/46/EC, such as, in particular, with respect to the EU Standard Contractual Clauses or similar transfer mechanisms, Company may request reasonable changes or additions to this Addendum to reflect applicable requirements.

C. Third party beneficiary clause

The parties agree that affiliates of the Company shall be entitled under and can enforce the terms of this Addendum against Supplier as third-party beneficiaries.

D. Termination

In the event of Supplier's violation of any obligation under Data Protection Laws or this Addendum, Company, without prejudice to any other rights which it may have, shall be entitled to terminate any Services Agreement forthwith. Any terms of this Addendum that by their nature extend beyond the termination of the Services Agreement, including without limitation this Addendum, Section A(i), shall remain in effect.

E. Precedence

In the event of a conflict between this Addendum and other provisions of the Services Agreement, this Addendum shall prevail.

[Signature page follows.]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed as of _____, ___, 20___ by their respective officers thereunto duly authorized.

COMPANY:
VigiLife, Inc.

By:
Name:
Title:

SUPPLIER:

_____

By:
Name:
Title:

Exhibit 1 to Data Protection Addendum

Description of Processing

A. Subject-matter, nature and purpose of the Processing

Supplier provides certain services to Company, including *[insert general description of services relating to processing of personal data]*, as further specified in the Services Agreement. In the context of performing the obligations under the Services Agreement, Supplier may Process

certain of Company's Personal Data as necessary for the purposes of *[insert purposes of Processing]*, as further specified in the Services Agreement. Such processing may include:
[insert description of relevant data processing activities/operations].

B. Duration of the Processing

[insert duration of data processing, e.g.: "The agreed Processing of Personal Data shall commence upon the effective date of the Services Agreement and be carried out for the term of the Services Agreement. The services relating to Processing of Personal Data shall automatically end in case the Services Agreement is effectively terminated or expires, in which case the Personal Data shall be handled in accordance with Section A(i). To the extent the Processing of Personal Data by Supplier is necessary for the winding-up of the Services Agreement, e.g. with respect to returning the Personal Data, the provisions of Section A shall continue to apply until the completion of the winding-up."]

C. Categories of Data Subjects

The Processing will concern the following categories of Data Subjects:
[insert categories of data subjects concerned, e.g.: a. Company employees and job candidates b. Managers, employees, agents or other contact persons at business partners c. Company customers that are natural persons d. Patients, research subjects or other customers of Company's clients]

D. Types of Personal Data

The Processing will concern the following types of Personal Data *[insert types of Personal Data concerned, e.g.:]*

- **a) Company employees and job candidates:**
  name, contact details (address, phone number and direct line, e-mail address), birth date/ country, gender, education (e.g., highest education level, country, degree, certificates), job information about current and previous employment (position, kind of work, work location, salary, replacement, company, location, department, position, function, grade, supervisor, employee class, grade and labor start/ entry date, labor agreement, business title, full or part-time, shifts, working hours), professional skills, CV and resume, training, compensation and remuneration (e.g., compensation rate, salary, target bonus, incentives, benefits), individual development plan, performance goals and assessment, position in company, bank account number and corporate credit card number, national ID and social security number, information about an immigration background.
- **b) Managers, employees, agents or other contact persons at business partners:**
  contact details (name, address, phone number and direct line, e-mail address).
- **c) Company customers that are natural persons:**
  name, contact details (address, phone number and direct line, e-mail address), information regarding purchases of such customers, bank account details, credit information, information about such customers' interest in Company products.
- **d) Patients, research subjects or other customers of Company's clients:**
  [insert the type of data in this category that your service providers might handle]

The Processing will concern the following special categories of data[^1] :
[...]

The Processing will include Personal Data relating criminal convictions and offenses relating to:
[...]

[^1] : *"Special categories of data" means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.*

HIPAA Mappings to VigiLife Policies and Controls

2024.02.13

Below is a list of HIPAA Safeguards and Requirements and the VigiLife policies and controls in place to meet those.

HIPAA Administrative Controls	VigiLife Policies and Controls
Security Management Process - 164.308(a)(1)(i)	Risk Management
Assigned Security Responsibility - 164.308(a)(2)	Roles and Responsibilities
Workforce Security - 164.308(a)(3)(i)	HR & Personnel Security
Information Access Management - 164.308(a)(4)(i)	Access Policy; Data Management; and Data Protection
Security Awareness and Training - 164.308(a)(5)(i)	Roles and Responsibilities Policy; and HR & Personnel Security
Security Incident Procedures - 164.308(a)(6)(i)	Threat Detection and Prevention; and Incident Response
Contingency Plan - 164.308(a)(7)(i)	Business Continuity and Disaster Recovery

HIPAA Administrative Controls	VigiLife Policies and Controls
Contingency Plan - 164.308(a)(7)(i)	Business Continuity and Disaster Recovery
Evaluation - 164.308(a)(8)	Compliance Audits and System Audits

HIPAA Physical Safeguards	VigiLife Policies and Controls
Facility Access Controls - 164.310(a)(1)	Facility and Physical Security
Workstation Use - 164.310(b)	Access Policy and HR & Personnel Security
Workstation Security - 164.310('c')	Access Policy and HR & Personnel Security
Device and Media Controls - 164.310(d)(1)	Mobile Device Security and Disposable Media Management; Data Management; and Data Protection

HIPAA Technical Safeguards	VigiLife Policies and Controls
Access Control - 164.312(a)(1)	Access Policy
Audit Controls - 164.312(b)	Compliance Audits and System Audits
Integrity - 164.312('c')(1)	Access Policy; Compliance Audits and System Audits; and Threat Detection and Prevention
Person or Entity Authentication - 164.312(d)	Access Policy
Transmission Security - 164.312(e)(1)	Access Policy; Data Management; and Data Protection

HIPAA Organizational Requirements	VigiLife Policies and Controls
Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i)	Business Associate Agreements; Vendor Management

HIPAA Policies and Procedures and Documentation Requirements	VigiLife Policies and Controls
Policies and Procedures - 164.316(a)	Policy Management
Documentation - 164.316(b)(1)(i)	Policy Management

HITECH Act - Security Provisions	VigiLife Policies and Controls
Notification in the Case of Breach - 13402(a) and (b)	Breach Notification
Timelines of Notification - 13402(d)(1)	Breach Notification
Content of Notification - 13402(f)(1)	Breach Notification

NIST Mappings to VigiLife Policies and Controls

2024.02.13

Below is a list of NIST SP 800-53 Controls Families and the mappings to VigiLife policies and controls in place.

ID	NIST SP 800-53 Control Family	VigiLife Policies and Controls
AC	Access Control	[Access][1]
AT	Awareness and Training	[Roles and Responsibilities][2]
AU	Audit and Accountability	[Roles and Responsibilities][2]; [Compliance Audits][3]

ID	NIST SP 800-53 Control Family	VigiLife Policies and Controls
CA	Security Assessment and Authorization	[Risk Management][4]; [Access][1]
CM	Configuration Management	[Configuration and Change Management][5]
CP	Contingency Planning	[Business Continuity and Disaster Recovery][6]
IA	Identification and Authentication	[Access][1]
IR	Incident Response	[Incident Response][7]; [Breach Notification][8]
MA	Maintenance	[Configuration and Change Management][5]
PE	Physical and Environmental Protection	[Facility and Physical Security][9]
PL	Planning	[Security Program Overview][10]; [Security Architecture & Operating Model][11]
PS	Personnel Security	[HR & Personnel Security][12]
RA	Risk Assessment	[Risk Management][4]
SA	System and Services Acquisition	[Third Party Security, Vendor Risk Management and Systems/Services Acquisition][13]
SC	System and Communications Protection	[Data Management][14]; [Data Protection][15]; and [Threat Detection & Prevention][16]
SI	System and Information Integrity	[Data Management][14]; [Data Protection][15]; [Product Security & Secure Software Development][17]; [Vulnerability Management][18];and [System Audits, Monitoring & Assessments][19]
PM	Program Management	[Security Program Overview][10]; [Roles and Responsibilities][2]; and [Policy Management][20]
[1] :/access/		
[2] :/rar/		
[3] :/compliance-audit/		
[4] :/risk-mgmt/		
[5] :/ccm/		
[6] :/bcdr/		

ID	NIST SP 800-53 Control Family	VigiLife Policies and Controls
[7] :/ir/		
[8] :/breach/		
[9] :/facility/		
[10] :/program/		
[11] :/model/		
[12] :/hr/		
[13] :/vendor/		
[14] :/data-mgmt/		
[15] :/data-protection/		
[16] :/threat/		
[17] :/sdlc/		
[18] :/vuln-mgmt/		
[19] :/system-audit/		
[20] :/policy-mgmt/		