Krengel Technology HIPAA Policies and Documentation

The Krengel Technology HIPAA Policy

Purpose and Scope

This document was developed by referencing documentation provided by the Office of Civil Rights and the U.S. Government Printing Office.

Krengel Technology is required by the Health Insurance Portability and Accountability Act (HIPAA) to ensure the privacy and security of all "Protected Health Information" or "PHI" received, maintained, or transmitted by or for its Business Associates. This Policy is intended to guide and educate all team members at Krengel Technology.

What is Protected Health Information (PHI) and What is Not

What is PHI?

Protected Health Information (PHI) is any individually identifiable health information that can be linked to a particular person. It includes all information that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. This information can relate to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or,
- The past, present, or future payment for the provision of health care to the individual.

Data elements commonly used to link health information to a specific individual are called the HIPAA identifiers (details provided below).

What is not PHI?

Health information that does not identify an individual or that cannot be used to identify an individual is not PHI, but great rigor is required to confirm that no identifier is present in the dataset. For example, a dataset of vital signs by themselves do not constitute Protected Health Information. However, if the vital signs dataset includes medical record numbers, then the entire dataset must be protected since it contains an identifier.

There are some types of identifiable health information that are not protected as PHI under HIPAA:

- Information in employment records
- Information about an individual who has been deceased for more than 50 years

The List of 18 Protected Health Information identifiers

The following data elements have been specifically identified in the regulation as being “identifiers.” When a medical record or result contains or is associated with any of these elements, it may be traceable back to the person associated with that record.

Any document or communication containing health information created, received, maintained, or transmitted by or for any of the HIPAA Covered Components is covered by HIPAA if it includes any of these elements:

1. Names (including initials only);
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by an investigator to code the data)

The Difference Between Privacy and Security

HIPAA contains both a Privacy Rule and a Security Rule. Security and privacy are distinct, but go hand-in-hand.

Privacy basically relates to *the right* of an individual to *control* the use of his or her personal information. Protected Health Information (PHI) should not be divulged or used by others without the patient’s authorization, except in certain limited circumstances (for example, to confer with a referring physician). The HIPAA Privacy Rule covers the confidentiality of PHI in *all forms and formats* including electronic, paper and oral. Confidentiality is an assurance that the information will be safeguarded from unauthorized use and disclosure.

Security is *a mechanism* used to protect the privacy of information. The HIPAA Security Rule focuses on administrative, technical and physical safeguards specifically as they relate to *electronic* PHI (ePHI). Protection of ePHI data from unauthorized access, alteration, loss or destruction, whether external or internal, stored or in transit, is all part of the HIPAA Security Rule.

HIPAA Security

This document lists all the security controls defined and required by HIPAA. The policies that govern how Krengel Technology meets these requirements are also provided as part of the checklist. The HIPAA Privacy and Security Officers at Krengel Technology are all available to assist the employees in this effort.

Krengel Technology has entered into an AWS Customer Agreement [http://aws.amazon.com/agreement] with Amazon Web Services, Inc., including an AWS BUSINESS ASSOCIATE ADDENDUM [http://www.krengeltech.com/documents/KrengelTechnologyInc-AWSBusinessAssociateAddendum.pdf] (“Amazon Agreements") governing HIPAA accounts as defined therein. All "HIPAA Accounts" hosted using the Amazon Web Services, Inc. are governed by the Amazon Agreements

Required vs. Addressable

Note that the controls are classified with an “R” for “required” or an “A” for “addressable”. For example, Risk Analysis is followed by ***R*** *– § 164.308(a)(1)(ii)(A)*. If the control is required, no system can be approved to contain or process HIPAA information unless this control is in place. If the control is “addressable”, the organization must respond in one of three ways and must document its decision. The decision to be taken will be made jointly by the organization and Information Security during the required Risk Assessment.

1. Implement the addressable implementation specifications. This must be done if it is reasonable and appropriate to do so. Otherwise,
2. Implement one or more alternative security measures to accomplish the same purpose if there is a reasonable and appropriate alternative. Otherwise,
3. Not implement either an addressable implementation specification or an alternative.

The decision will depend on a variety of factors, such as, among others, the entity’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions must be documented in writing and should include the factors considered as well as the results of the risk assessment on which the decision was based.

Business Associates & Business Associate Agreements

A **Business Associate** is defined in HIPAA as a person or organization that is not a member of the Covered Component’s (or support unit’s) Workforce and that falls within one of the following categories:

- on behalf of the Covered Component (or support unit), it creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA, including billing, claims processing or administration, data analysis, process or administration, utilization review, quality assurance, patient safety activities, benefit management, or practice management;

or

- it provides one of the following types of services to the Covered Component where the service involves the disclosure of PHI to the business associate by the Covered Component or another business associate. The types of services are: legal, actuarial or accounting, consulting, data aggregation, management or administrative, accreditation, or financial services.

Administrative Safeguards

§ 164.308(a)(1) Security Management Process

Implement policies and procedures to prevent, detect, contain and correct security violations. § 164.308(a)(1)

- Krengel Technology will protect the confidentiality, integrity, and availability of ePHI by maintaining appropriate safeguards for the networks and systems that handle ePHI.
- The Krengel Technology HIPAA Security Officer(s) are responsible for the development and maintenance of policies and procedures designed to prevent, detect, contain and correct security violations.
- Team members wishing to receive, store, process, or transmit ePHI must adhere to the requirements found in the Krengel Technology HIPAA Policies document (this document). No computer system, network, electronic device or software may contain ePHI until the proper Risk Analysis has been completed and the solution is approved by the Krengel Technology Security Officer. PHI is only allowed in PHI-Approved systems.

§ 164.308(a)(1)(ii)(A) Risk Analysis

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information held by the Covered Entity. R – § 164.308(a)(1)(ii)(A)

The Krengel Technology Information Security department is responsible for the development and maintenance of the HIPAA Assessment and Approval process.

Krengel Technology provides customer-specific solutions to their clients. Clients often provide Krengel Technology with a subset of sample data to develop against to achieve optimum results. When sample data contains electronic Protected Health Information (ePHI), Krengel Technology has policies and procedures in place to ensure ePHI is handled in accordance with HIPAA regulation(s).

Potential Risks/Vulnerabilities

Data Center

Potential risks/vulnerabilities include:

- Server-component failure
- Network component failure
- Unauthorized physical access to data center

- Network connectivity or “up-time”

Data Transfer

Potential risks/vulnerabilities include:

- Unsecure/unencrypted data connection
- Transmitting a user's credentials to Krengel Technology’s secure file transfer site.

Server Security

Potential risks/vulnerabilities include:

- Unauthorized virtual/physical access
- Harmful virus

§ 164.308(a)(1)(ii)(B) Risk Management

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a). R – § 164.308(a)(1)(ii)(B)

The Krengel Technology Information Security department has identified and analyzed potential risks/vulnerabilities. Potential risks/vulnerabilities are managed and addressed below.

Data Center

Krengel Technology has a redundant data center configuration with fail-over functionality for power supply, network connectivity, and servers.

Data Transfer

Krengel Technology will only accept ePHI, as a Business Associate, through Krengel Technology’s Secure File Transfer (SSH over FTP or SFTP) server. SFTP users are created with a unique username, strong password, and unique directory. Usernames and passwords are never sent to the SFTP user in the same email (passwords are prefered to be sent via SMS).

Server Security

Virtual access to Krengel Technology’s data center is guarded by an edge-network security device/software requiring multi-factor authentication. Once an approved team member has authenticated to the network and to the private subnet, virtual volumes that house ePHI are encrypted while at rest, and require authorized users to authenticate to decrypt before being able to use ePHI for development. Virtual Sessions and virtual volumes will both automatically disconnect after a predetermined time of idle activity.

Physical Access to the Krengel Technology’s data center (specifically servers housing ePHI) is restricted and requires a key to gain access. Only authorized members of the Information Security team have access to these servers.

§ 164.308(a)(1)(ii)(C) Sanction Policy

Apply appropriate sanctions against Workforce members who fail to comply with the security policies and procedures of the Covered Entity. R – § 164.308(a)(1)(ii)(C)

Krengel Technology observes a “three-strike” rule for disciplinary action for team members who fail to comply with security policies. Formal notices will be given for each incident. Disciplinary action taken beyond what is outlined in this document is the sole discretion of the Information Security department.

- First incident - team member will required to re-review Krengel Technology’s HIPAA Training documentation and demonstrate their understanding of the subject matter.
- Second incident - A probation period will be issued. The team member will remain on probation until they review Krengel Technology’s HIPAA Training documentation and demonstrate their understanding of the subject matter.
- Third incident - Disciplinary action will be decided by the Information Security Department.

§ 164.308(a)(1)(ii)(D) Information System Activity Review

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. R – § 164.308(a)(1)(ii)(D)

The Krengel Technology Security Officer will review system activity, audit logs, access reports and security incident tracking reports on a weekly basis. Notifications

§ 164.308(a)(2) Assigned Security Responsibility

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the Covered Component or business associate. R – § 164.308(a)(2)

The Krengel Technology HIPAA Security Officer and Privacy Officer is: Nathan Bartell.

Responsibilities:

- Ensure that the necessary and appropriate HIPAA related policies are developed and implemented to ensure that PHI is properly used and disclosed (privacy) and to safeguard the integrity, confidentiality, and availability of ePHI (security).
- Act as a spokesperson and single point of contact for Krengel Technology in all issues related to HIPAA security and privacy
- Provide training to staff on HIPAA Compliance.

§ 164.308(a)(3) Workforce Security

Implement policies and procedures to ensure that all members of its Workforce have appropriate access to electronic Protected Health Information, and to prevent those Workforce members who do not have access under from obtaining access to electronic Protected Health Information. R – § 164.308(a)(3)

Electronic access to ePHI is granted and monitored on an individual basis. Once a team member has been granted access, they will be required to register a smart device (ie smartphone) or request a hardware passcode generator, to use for multi-factor authentication which is required to gain access to ePHI. team members who have not completed these steps will are considered unauthorized and will not have access to ePHI.

§ 164.308(a)(3)(ii)(A) Authorization and/or Supervision

Implement procedures for the authorization and/or supervision of Workforce members who work with electronic Protected Health Information or in locations where it might be accessed.A – § 164.308(a)(3)(ii)(A)

Krengel Technology team members are trained extensively in securely handling PHI. When an authorized team member starts a remote session into a PHI zone, the activity is logged in detail. The session has mechanisms in place to protect PHI-data from leaving the secure environment.

§ 164.308(a)(3)(ii)(B) Workforce Clearance Procedure

Implement procedures to determine that the access of a Workforce member to electronic Protected Health Information is appropriate. A – § 164.308(a)(3)(ii)(B)

When a Krengel Technology team member is assigned to a project that contains ePHI, that team member will require access to all ePHI sample data. If a Krengel Technology team member is not assigned to a project, access to ePHI is not available.

Often when working on projects, team members need support from other team members to serve as “a second set of eyes”. In this case, team members still need to fill out an Access Authorization Request form.

§ 164.308(a)(3)(ii)(C) Termination Procedures

Implement procedures for terminating access to electronic Protected Health Information when the employment or engagement of a Workforce member ends or as required by determinations made in accordance with the Workforce clearance procedures. A – § 164.308(a)(3)(ii)(C)

In order to properly remove access to ePHI from team members when their employment or engagement ends or when the access is no longer appropriate, Krengel Technology uses the following process. The process includes:

- Internal notification to ensure that the appropriate personnel are made aware that the user’s access to ePHI is no longer required.
- Recovery of all forms of access to PHI that was granted or assigned to that user. Examples include, but are not limited to, keys, access tokens, and identification badges.
- Disabling the user’s accounts on networks and systems.
- Changing administrative or other shared passwords of which the user has been made aware.

If account access must be immediately revoked, email infosec@krengeltech.com.

§ 164.308(a)(4) Information Access Management

Implement policies and procedures for authorizing access to electronic Protected Health Information that are consistent with the applicable requirements in the Privacy Rule. R – § 164.308(a)(4)

This policy ensures that team members needing access to ePHI have appropriate access, and provides procedural safeguards to ensure that access to ePHI is properly restricted.

Before access to ePHI can be provided to a user, that user must be authorized for the appropriate minimum level of access that their position requires. Access to ePHI and systems that store or process ePHI requires a valid and authorized user account and password. Users are required to use multi-factor authentication (MFA) to authenticate themselves to these systems using their unique user accounts.

§ 164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Functions

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic Protected Health Information of the clearinghouse from unauthorized access by the larger organization. R – § 164.308(a)(4)(ii)(A)

Not applicable. Krengel Technology performs no clearinghouse functions.

§ 164.308(a)(4)(ii)(B) Access Authorization

Implement policies and procedures for granting access to electronic Protected Health Information, for example, through access to a workstation, transaction, program, process, or other mechanism. A – § 164.308(a)(4)(ii)(B)

- All ePHI will reside in Krengel Technology's Secure Data Center.
- Access to ePHI can only be granted by the Security Officer after an Access Authorization Form request has been completed and submitted.
- Access will be limited to authorized team members
- Modification or termination of ePHI access needs to be communicated by an Access Authorization Form.

§ 164.308(a)(4)(ii)(C) Access Establishment and Modification

Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. A – § 164.308(a)(4)(ii)(C)

Each system containing ePHI must have one or more security administrators who will be responsible for controlling access to the ePHI once such access has been authorized in writing. All new access requests, modifications, and authorizations for such requests will be documented on an Access Authorization Form.

- The security officer is responsible for establishing, modifying, and removing access to the ePHI maintained in the system based upon proper documented authorization as well as maintaining the Access Authorization Form documenting the specific level of access granted.
- Once access has been granted, the security officer will keep the approved Access

Authorization Form on file for a minimum of six years from the time access is terminated [164.316(b)(2)(i)].

- Occasionally a user's required access may change. Managers and supervisors may request access modifications for a user. Such requests for changes will be submitted on the Access Authorization Form.
- Managers and supervisors will notify the security officer immediately when a user's employment or term of engagement has terminated or when the current level of access to ePHI is no longer required. This notice may be via e-mail or any other expedient method, but it must be in writing.
    - The security officer will be responsible for ensuring that access is removed within 48 hours of receiving the written request. In the event of involuntary termination or in other special circumstances, access may need to be removed immediately.
- The security officer will review user access levels on an annual basis to ensure that they are appropriate and certify to the HIPAA Security Officer that such reviews have occurred.

§ 164.308(a)(5) Security Awareness and Training

Implement a security awareness and training program for all members of its Workforce (including management). R – § 164.308(a)(5)

All team members must complete the security awareness and training program. The security awareness training covers:

- What HIPAA is and why Krengel Technology needs to be compliant.
- What PHI is and how to identify PHI.
- Policies and procedures for working with PHI.
- Policies and procedures for identifying and reporting a security breach.

Completion of the training program is required before access can be granted to ePHI. Krengel Technology Information Security has developed training documentation on HIPAA Privacy and Security. The security awareness and training program will be updated from time to time and new versions may be used to meet the security reminder requirement.

§ 164.308(a)(5)(ii)(A) Security Reminders

Periodic security awareness updates. A – § 164.308(a)(5)(ii)(A)

The Krengel Technology Security Officer is responsible for issuing periodic security and awareness updates to the entire team.

§ 164.308(a)(5)(ii)(B) Protection from Malicious Software

Procedures for guarding against, detecting, and reporting malicious software. A – § 164.308(a)(5)(ii)(B)

Only approved software will be allowed on systems that house ePHI (see Approved Software). Systems that store ePHI will be required to have monitoring software installed. Monitoring software will need to be

approved by the Security Officer.

§ 164.308(a)(5)(ii)(C) Log-in Monitoring

Procedures for monitoring log-in attempts and reporting discrepancies. A – § 164.308(a)(5)(ii)(C)

Krengel Technology utilizes a edge-network security device and software that logs the following:

- Timestamp
- User
- Server/Data being accessed
- IP Address
- Access Success/Failure
- As well as many additional details about the session.

§ 164.308(a)(5)(ii)(D) Password Management

Procedures for creating, changing, and safeguarding passwords.

Strong passwords are required for any account that has access to ePHI. A strong password is defined as being at least 7 characters long and containing at least three of the following:

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

Strong passwords should also:

- not contain a word found in a dictionary
- not contain common, easy obtained information about the individual (pets names, address, etc)
- be kept private to the individual

§ 164.308(a)(6) Security Incident Procedures

Implement policies and procedures to address security incidents. R – § 164.308(a)(6)

When a Security incident has been identified, the team member should immediately fill out a Security Incident report and/or contact the Security Officer at infosec@krengeltech.com.

§ 164.308(a)(6)(ii) Response and Reporting

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Covered Entity; and document security incidents and their outcomes. R – § 164.308(a)(6)(ii)

Members of the team are trained to identify and understand a security incident in accordance with HIPAA

regulations and are responsible for reporting known or suspected security issues. The Security Officer is responsible for responding to incidents in accordance with established procedures.

§ 164.308(a)(7) Contingency Plan

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic Protected Health Information. R – § 164.308(a)(7)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the primary data set, a contingency plan is not necessary. A contingency plan for vandalism is met by the Physical Safeguards.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.308(a)(7)(ii)(A) Data Backup Plan

Establish and implement procedures to create and maintain retrievable exact copies of electronic Protected Health Information. R – § 164.308(a)(7)(ii)(A)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the primary data-set, this is not necessary.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.308(a)(7)(ii)(B) Disaster Recovery Plan

Establish (and implement as needed) procedures to restore any loss of data. R – § 164.308(a)(7)(ii)(B)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the primary data-set, a natural disaster is not necessary.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.308(a)(7)(ii)(C) Emergency Mode Operation Plan

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic Protected Health Information while operating in emergency mode. R – § 164.308(a)(7)(ii)(C)

Because the nature of Krengel Technology's use with ePHI, and that it is a sample-set or copy and not the primary data-set, this is not necessary.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.308(a)(7)(ii)(D) Testing and Revision Procedures

Implement procedures for periodic testing and revision of contingency plans. (The three plans above.) A – § 164.308(a)(7)(ii)(D)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the primary data set, a contingency plan for natural disaster is not necessary.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis

Assess the relative criticality of specific applications and data in support of other contingency plan components. A – § 164.308(a)(7)(ii)(E)

Because the nature of Krengel Technology's use with ePHI, and that it is a sample-set or copy and not the primary data-set, this is not necessary.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.308(a)(8) Evaluation

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic Protected Health Information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule]. R – § 164.308(a)(8)

Systems that have been approved for ePHI will be reviewed every two years to ensure their continued compliance with the policies. At the same time, or upon the initiative of an involved party, the Krengel Technology HIPAA policy (this document) may also be evaluated to ensure continued viability in light of technological, environmental, or operational changes that could affect the security of electronic Protected Health Information.

Physical Safeguards

§ 164.310(a)(1) Facility Access Controls

Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. R – § 164.310(a)(1)

Physical access to Krengel Technology data centers is limited to authorized Krengel Technology employees. Physical access logs containing detailed information will be in an electronic log file. Authorized users are

required to manually log their name and reason for accessing server.

§ 164.310(a)(2)(i) Contingency Operations

Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. A – § 164.310(a)(2)(i)

Because the nature of Krengel Technology's use with ePHI data being a sample-set and not the primary data set, a contingency disaster recovery plan is not necessary.

§ 164.310(a)(2)(ii) Facility Security Plan

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. A – § 164.310(a)(2)(ii)

Physical access to Krengel Technology data centers is limited to authorized Krengel Technology team members. Physical access logs containing detailed information will be housed on-site in hard copy, as well as in an electronic log file. Authorized users are required to manually log their name, date, time, and reason for accessing server.

§ 164.310(a)(2)(iii) Access Control and Validation Procedures

Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. A – § 164.310(a)(2)(iii)

Physical access to Krengel Technology PHI zones require a key. Only authorized Krengel Technology team members have a key to gain access to PHI zones.

§ 164.310(a)(2)(iv) Maintenance Records

Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). A – § 164.310(a)(2)(iv)

All modifications to physical components of Krengel Technology data centers are documented in the Krengel Technology Access Log.

§ 164.310(b) Workstation Use

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific

workstation or class of workstation that can access electronic protected health information. R – § 164.310(b)

Authorized Krengel Technology team members' access to ePHI will be facilitated through a remote desktop session. Regardless of the device used to connect, the connected session has restrictions in place that prevent ePHI from leaving the isolated ePHI zone.

§ 164.310(c) Workstation Security

Implement physical safeguards for all workstations that access electronic Protected Health Information, to restrict access to authorized users. R – § 164.310(c)

Krengel Technology workstation computers do not have direct access to any ePHI. In order to gain access to the private subnet where ePHI resides, authorized users need to use multi-factor authentication to log in. Once authenticated into the secure environment, authorized users will also need to provide credentials to decrypt the virtual volumes that house ePHI data.

§ 164.310(d)(1) Device and Media Controls

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Protected Health Information into and out of a facility, and the movement of these items within the facility. R – § 164.310(d)(1)

All ePHI must be permanently removed from any electronic device (hard drive, storage system, removable disk, floppy drive, CD ROM, DVD, PCMCIA card, memory sticks, and all other forms of media and storage devices.) before the devices can be discarded or re-used. Permanently removing data from electronic device is done by a process called "wiping". Krengel Technology utilizes a 7-pass cycle wiping process.

§ 164.310(d)(2)(i) Disposal

Implement policies and procedures to address the final disposition of electronic Protected Health Information, and/or the hardware or electronic media on which it is stored. R – § 164.310(d)(2)(i)

When ePHI is received into Krengel Technology's secure data center, it is placed in a virtual drive and uses on-the-fly encryption to ensure integrity and security during the life of the project. Once the project is over, the virtual drive is decommissioned using a 7-pass cycle wipe to ensure all ePHI has been completely disposed.

§ 164.310(d)(2)(ii) Media Re-use

Implement procedures for removal of electronic Protected Health Information from electronic media before the media are made available for re-use. R – § 164.310(d)(2)(ii)

Krengel Technology has strict policies where ePHI can reside. Electronic media that is approved by the Security Officer for re-use goes through a 7-pass cycle data cleansing process to ensure optimal removal.

§ 164.310(d)(2)(iii) Accountability

Maintain a record of the movements of hardware and electronic media and any person responsible therefore. A – § 164.310(d)(2)(iii)

All Krengel Technology hardware that stores or transmits ePHI is inventoried and tracked electronically by the Krengel Technology Security Officer in the PHI Hardware Log.

§ 164.310(d)(2)(vi) Data Backup and Storage

Create a retrievable, exact copy of electronic Protected Health Information, when needed, before movement of equipment. A – § 164.310(d)(2)(vi)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the primary data set, this objective is not necessary.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

Technical Safeguards

§ 164.312(a)(1) Access Control

Implement technical policies and procedures for electronic information systems that maintain electronic Protected Health Information to allow access only to those persons or software programs that have been granted access rights. R – § 164.312(a)(1)

Krengel Technology houses ePHI in private subnet. Authorized users are able to access this information by connecting to the edge-network security device. The edge device requires multi-factor authentication, and authorized employees need to enter a secret code that refreshes every 30 seconds, in addition to a username and strong password.

§ 164.312(a)(2)(i) Unique User Identification

Assign a unique name and/or number for identifying and tracking user identity. R – § 164.312(a)(2)(i)

All authorized users will authenticate to the edge-network device with their unique username/password and multi-factor authentication code. Krengel Technology has a best practice of using first initial and last name combinations for keeping usernames unique and easily readable to humans.

§ 164.312(a)(2)(ii) Emergency Access Procedure

Establish (and implement as needed) procedures for obtaining necessary electronic Protected Health Information during an emergency. R – § 164.312(a)(2)(ii)

Not applicable. Krengel Technology houses data only for testing and development.

§ 164.312(a)(2)(iii) Automatic Logoff

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. A – § 164.312(a)(2)(iii)

There are two automatic logoff features that Krengel Technology utilizes to ensure idle sessions are disconnected.

After five minutes of inactivity, idle sessions in the Krengel Technology ePHI data center will automatically log off. After 60 minutes of idle read/write activity on the encrypted volumes, the volumes will automatically disconnect, requiring authorized users to re-authenticate to access encrypted volumes.

§ 164.312(a)(2)(iv) Encryption and Decryption

Implement a mechanism to encrypt and decrypt electronic Protected Health Information. (This item refers to data at rest. Data in motion is covered by Transmission Security.) A – § 164.312(a)(2)(iv)

Krengel Technology utilizes on-the-fly encryption to encrypt and decrypt all ePHI data.

§ 164.312(b)(1) Audit Controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic Protected Health Information. R – § 164.312(b)(1)

Krengel Technology utilizes an edge-network security device that requires multi-factor authentication to gain access to ePHI. All access activity is logged and archived.

§ 164.312(c)(1) Integrity

Implement policies and procedures to protect electronic Protected Health Information from improper alteration or destruction. R – § 164.312(c)(1)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the authoritative data set, this does not apply.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.312(c)(2) Mechanism to Authenticate ePHI

Implement electronic mechanisms to corroborate that electronic Protected Health Information has not been altered or destroyed in an unauthorized manner. A – § 164.312(c)(2)

Because the nature of Krengel Technology's use with ePHI data being a sample-set or copy and not the authoritative data set, this does not apply.

The responsibility of data integrity and redundancy of the primary data set belongs to the Covered Entity.

§ 164.312(d)Person or Entity Authentication.

Implement procedures to verify that a person or entity seeking access to electronic Protected Health Information is the one claimed. R – § 164.312(d)

Krengel Technology requires multi-factor authentication to safeguard access to ePHI. Security tokens are refreshed every 30 seconds and are retrieved by a security token device belonging to authorized users. Each authorized user has their own unique security token and device.

§ 164.312(e)(1) Transmission Security

Implement technical security measures to guard against unauthorized access to electronic Protected Health Information that is being transmitted over an electronic communications network. R – § 164.312(e)(1)

It is a policy of Krengel Technology that it will only accept ePHI from it's Business Associates to the secure data center through secure file transfer protocol (SSH over FTP) providing encryption while in transmission. Each SFTP user has an isolated directory that they have the ability to securely send files to. User credentials are created by Krengel Technology and are provided to the user in separate forms of communication (usernames can be emailed, but passwords are sent by SMS or verbally given to the end user).

§ 164.312(e)(2)(i) Integrity Controls

Implement security measures to ensure that electronically transmitted electronic Protected Health Information is not improperly modified without detection until disposed of. A – § 164.312(e)(2)(i)

Because the nature of Krengel Technology's use with ePHI data being a sample-set and not the authoritative data set, this does not apply.

§ 164.312(e)(2)(ii) Encryption

Implement a mechanism to encrypt electronic Protected Health Information whenever deemed appropriate. A – § 164.312(e)(2)(ii)

Krengel Technology utilizes SFTP (SSH over FTP) for encryption during ePHI data transmission, and

on-the-fly volume encryption for data at rest.

Organizational Requirements

§ 164.316(a) Policies and Procedures

Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A Covered Component or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. R – § 164.316(a)

This document meets this requirement for Krengel Technology.

§ 164.316(b)(1) Documentation

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. R – § 164.316(b)(1)

Formal policy documentation must be maintained to ensure that Krengel Technology team members have a clear understanding of management directives with respect to HIPAA compliance.

§ 164.316(b)(2)(i) Time Limit

Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. R – § 164.316(b)(2)(i)

If any change is made to any HIPAA policy the previous version of the policy must be archived and remain available for 6 years starting from when the new policy goes into effect.

- The Krengel Technology HIPAA Security Officer is responsible for maintaining historical copies of the enterprise policies.

§ 164.316(b)(2)(ii) Availability

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. R – § 164.316(b)(2)(ii)

- The HIPAA Security Officer is responsible for maintaining and promulgating enterprise policies.
- The Security Champion is responsible for maintaining and promulgating any policies established at

the Covered Component level.

§ 164.316(b)(2)(iii) Updates

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic Protected Health Information. R – § 164.316(b)(2)(iii)

The Krengel Technology HIPAA Policy (this document) will be evaluated when needed to ensure continued viability in light of technological, environmental, or operational changes that could affect the security of electronic Protected Health Information (ePHI).

The policy evaluation process may be triggered by one or more of the following events:

- Changes in the HIPAA Security Rule or Privacy Rule or other applicable law;
- Changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures;
- A material security violation, breach, or other security incident.