HIPAA –SECURITY RULE POLICIES AND PROCEDURES

Policies and Procedures for the:

18 Standards and 44 Implementation Specifications of the HIPAA Security Rule

Zoom RPM, LLC

4 Birdie Drive

Suffern, NY, 10901

Brian L Tuttle, CHP, CPHIT, CBRA, CHA, CISSP, CCNA

Personal and Confidential

Revision 1: June 2022

Table of Contents

HIPAA Security Rule: Administrative Safeguards

Standard: Assigned Security Responsibility

Implementation Specification: *Assigned Security Responsibility*

Assigned Security Responsibility		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Assigned Security Responsibility	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(A)	Required

Requirement: Identify the security official who is responsible for developing and implementing the policies and procedures required by the Security Rule for the protection of electronic health information.

Policy: Our business will designate a security official to be the “go to” person who will have overall responsibility to protect the confidentiality, integrity, and availability of protected health information and to guide our business through compliance activities and meet relevant standards and regulations.

Procedures: We have designated Jonathan Cohen (Chief Operating Officer) to be our HIPAA Security Official.

The Security Official may allocate out duties to the appropriate internal resources as needed.

Our Security Official is the “go-to” for any compliance questions or issues, including:

- Developing and implementing security policies and procedures in accordance with the HIPAA Security Rule and all other applicable laws;
- Providing leadership and assume accountability for compliance with the HIPAA Policies and Procedures related to security;
- Coordinating risk assessment and risk management activities to ensure ongoing identification of threats to the confidentiality, integrity and availability of PHI and selection of appropriate safeguards to manage and reduce risks;
- Ensuring that operations comply with policies and procedures related to security and that security policies, procedures, and

practices are revised as needed;

- Reviewing and investigating all security incidents and ensuring that response and reporting procedures are followed and that harm caused by security incidents is mitigated to the extent practicable;
- Cooperating with oversight agencies in any investigations of security violations;
- Developing and conducting training on and fostering awareness of security policies and procedures to ensure that all members of the workforce, including management, receive adequate and appropriate security training;
- Ensuring that all documentation required by the HIPAA Security Rule is created and maintained for six years from the date it was created or was last in effect, whichever is later;
- Serving as an internal and external liaison and resource with outside entities (including business associates, technology vendors, trustees, and other parties) to ensure that security practices are implemented, consistent and coordinated.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Management Process

Implementation Specification: *Risk Analysis/Assessment*

Risk Analysis/Assessment		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security management process	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(A)	Required

Requirement: 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.

Policy: We will conduct a third party external or an internal HIPAA audit periodically to ensure our business is taking reasonable and appropriate actions regarding the security of electronic protected health information.

Procedure: We analyzed our weaknesses in business workflow and procedures, and consulted the risk analysis reports, audit comments, security requirements, and results of security assessment prior to completing our policies and procedures.

We identified any history of attacks, including those caused by natural disasters, disgruntled employees, water damage, electrical outages, viruses, HIPAA concerns, and current controls in place. Our findings are included in our risk assessment reports completed on June 16th, 2022 by outsourced consultant Brian L Tuttle with over 20 years of experience in health IT and HIPAA compliance.

We rated the likelihood of each risk, including potential contingencies and potential issues, on a scale of 1 to 5, with 1 being least likely and 5 being highly likely, and developed steps to mitigate the future likelihood of any potential risk.

**These policies and procedures were developed as a result of the risks we discovered in our risk analysis and the need to control and mitigate those risks and ensure all implementation specifications are addressed.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Management Process

Implementation Specification: *Sanction Policy*

Sanction Policy		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security management process	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(C)	Required

Requirement: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Policy: Our business has implemented a sanction policy to safeguard confidential health information in oral, written, and electronic forms. Workforce members are responsible for complying with our HIPAA Security policies and procedures as well as information contained within the confidentiality agreement. Failure to do so may result in disciplinary action, up to and including termination of employment.

Procedures: All workforce members including contracted employees who are privy to protected health information will receive training on our policies and procedures prior to adoption of new policies or modification of existing policies.

As part of new employee orientation, all new workforce members and contractors are trained for HIPAA, required to sign our HIPAA Confidentiality Agreement and abide by these written policies.

Sanctions: Any wrongful disclosure of private health information will lead to **immediate** termination of employee or breach of business associate agreement for our contractors.

If an employee wrongfully discloses private health information inadvertently, a warning will be issued. These measures are consistent with what is contained within our confidentiality agreement and covered within annual HIPAA training and onboarding training.

Any contractors working on our behalf are beholden to the bylaws contained within HIPAA as a “business associate”.

HIPAA Security Rule: Safeguards

Administrative

Standard: Security Management Process

Implementation Specification: *Information System Activity Review*

Information System Activity Review		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security management process	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(D)	Required

Requirement: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Policy: Our business will safeguard electronic protected health information and regularly review records of information activity, such as audit trails, system logs, access reports, and security incident tracking reports, for inappropriate use. Our business does not accept unauthorized snooping or peeking into any medical records, regardless of their public or private status.

We will impose sanctions on any workforce member who violates this policy.

Procedure: Our HIPAA Security Official or a designated member of the IT development team will be responsible for overseeing compliance of our policies and procedures by reviewing records of information system activity for inappropriate use on an “as needed” basis to ensure no inappropriate access is taking place within our cloud based software which houses protected health information or sensitive data.

As needed, a written account of audits is kept on within our *Access Monitoring Log* (on page 53 of this manual) indicating when the audit was done, what was audited, and who conducted

the audit.

Any of our staff members (or contractors) privy to protected health information (or sensitive data) are subject to system use auditing to ensure access to protected health information or any other sensitive data maintained by this business is appropriate.

HIPAA Security Rule: Safeguards

Administrative

Standard:

Workforce Security

Implementation Specification:

Authorization and/or Supervision

Authorization and/or Supervision		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Workforce security	68 Federal Register 8377 45 CFR 164.308 (a)(3)(ii)(A)	Addressable
Requirement: Implement policies and procedures to ensure that all workforce members have appropriate access to confidential health information and to prevent those workforce members who do not have access from obtaining it. **Policy:** Users are only granted the minimum necessary access to perform job function. This applies both to paper based private health information (PHI) access and electronic private health information access (ePHI) our clients maintain. **Procedure:** Our staff (and contractors) are only granted access to protected health information (PHI) based on the "minimum necessary" principle as set forth in the HIPAA/HITECH regulations. "Minimum necessary" means that our Security Official only grants access to staff or contractors for the specific areas within databases or applications needed to perform job function. Considering our business operates as a Software as a Service (SaaS), our developers and support may need full/admin access into the systems to perform job function. However, staff member (and contractor) access is only granted with final approval of the HIPAA Security Official and always based on the minimum necessary principle. In addition, user access into our system can be monitored via auditing capabilities of the systems hosting our software and the application itself.		

HIPAA Security Rule: Administrative Safeguards

Standard: Workforce Security

Implementation Specification: *Workforce Clearance Procedure*

Workforce Clearance Procedures		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Workforce security	68 Federal Register 8377 45 CFR 164.308 (a)(3)(ii)(B)	Addressable

Requirement: Determine that the access of a workforce member to confidential health information is appropriate.

Policy: At the security official's discretion or management, a background check will be authorized for any new employees or contractors.

Procedures: Our business analyzes job responsibilities of each workforce member or contractor on an individual basis.

Unless the staff member is already vetted per the judgement of the HIPAA Security Official, as part of our hiring procedures (and prior to granting any access to protected health information) we:

- Require a written application for employment and conduct a criminal background check for any staff member privy to protected health information
- Require proof of citizenship or resident alien status
- Confirm prior employment history
- Request professional/personal references and contact those references
- Confirm educational history and practicing credentials
- Confirm application statements, as appropriate.

HIPAA Security Rule: Administrative Safeguards

Standard: Workforce Security

Implementation Specification: *Termination Procedures*

Termination Procedures		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Workforce security	68 Federal Register 8377 45 CFR 164.308 (a)(3)(ii)(C)	Addressable

Requirement: Terminate access to confidential health information when the employment of a workforce member ends or as required by determinations made as part of our workforce clearance procedures.

Policy: It is our company policy to make every effort to preserve the relationship between employee and employer. We also acknowledge that there may be voluntary and involuntary reasons for termination of employment. Regardless of the cause, the employee's access to confidential health information will cease within **2 hours** of termination.

Procedures: We analyzed job responsibilities of workforce members and contractors. We incorporated those responsibilities into job descriptions prior to issuing a clearance for work on client systems. In the event those clearances change through termination of employment or contract, the following will occur:

- We will explain that authorization for access to electronic protected health information has changed and the user ID and password have been terminated
- We will follow the steps within our *termination checklist on page 57 of this manual*
- Workforce and contractors will be reminded of our sanction policy for a security incidents resulting from an unauthorized workforce member attempting to gain access to client protected health information, and of the potential criminal and civil penalties for a privacy breach or unauthorized disclosure of protected health information (even after

employment ends).

HIPAA Security Rule: Administrative Safeguards

Standard: Information Access Management

Implementation Specification: *Isolating Clearinghouse Functions*

Information Access Management		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Isolating Healthcare Clearinghouse Functions	68 Federal Register 8377 45 CFR 164.308 (a)(4)(ii)	Required
Requirement: Isolate Clearinghouse Functions Zoom RPM does not function as a clearinghouse in any way – no medical billing is performed		

HIPAA Security Rule: Administrative Safeguards

Standard: Information Access Management

Implementation Specification: *Access Authorization*

Access Authorization		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Information access management	68 Federal Register 8377 45 CFR 164.308 (a)(4)(ii)(B)	Required

Requirement: Authorize access to confidential health information consistent with your privacy rule.

Policy: Each workforce member is responsible for complying with our policies and procedures for accessing workstations, transactions, programs, processes, and other mechanisms used in the practice. Outside vendors who require access must be subject to the business associate agreement, with an obligation to comply with the Security Rule, as provided for in the HITECH Act provisions of the American Recovery and Reinvestment Act of 2009, signed into law by President Obama on February 17, 2009 and the provisions within the HIPAA Omnibus Rule of 2013.

Procedure: All access to our systems containing private health information is granted by the HIPAA Security Official or a designated member of the IT group and always based upon the minimum necessary standard as set forth in the HIPAA/HITECH regulation.

“Minimum necessary” means that our Security Official only grants access to staff (or contractors) for the specific areas within the database (or application) needed to perform job function.

Considering our business operates as a Software as a Service (SaaS) group, our developers and support staff may need full access into the systems to perform job function. However, staff member (and contractor access) is only granted with final approval of the HIPAA Security Official and user access is monitored via the auditing capabilities within the application and systems hosting the application.

HIPAA Security Rule: Administrative Safeguards

Standard: Information Access Management

Implementation Specification: *Access Establishment and Modification*

Establish and Modify Access		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Information access management	68 Federal Register 8377 45 CFR 164.308 (a)(4)(ii)(C)	Addressable

Requirement: Implement policies and procedures for how the workforce will be granted access (via workstation, transaction, program, or other mechanism).

Policy: Only persons authorized to modify electronic protected health information may do so.

Procedure: Each workforce member or contractor is granted the minimum amount of information necessary to complete assigned tasks, this is consistent with the minimum necessary standard as set forth within the HIPAA/HITECH regulations.

“Minimum necessary” means that our Security Official only grant access to staff or contractors for the specific areas within the database needed to perform job function.

Our HIPAA Security Official modifies user access “as needed” but not less than twice per year or as part of our termination checklist to ensure there are no unauthorized users within our system. If a user needs a higher level of access, a verbal request is made to the security official (or a member of the IT development group) and the access is approved or denied based on the HIPAA Security Official’s discretion.

Based upon risk and per the National Institute of Standard and Technologies (NIST), all access from staff members (and contractors) into the backend or frontend of the system requires a password of at least 8 characters “complex” and (for backend required/front end optional) an SSH key or a secondary pin (via smartphone) for two factor authentication.

This provides a two-tier level of access controls to protect our internal systems.

“Complex” meaning a number, symbol, and capital letter must be used.

See BYOD policy for personal devices.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Security Reminders*

Security Awareness and Training		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(i)	Addressable

Requirement: Implement a security awareness and training program for all members of the workforce (including management).

Policy: Securing our clients' protected health information is more than a policy; it is a primary responsibility of each workforce member who works for us.

Each workforce member and contractor is responsible for complying with these policies and procedures. To demonstrate our commitment to security we provide a HIPAA security awareness course once per year and upon employment.

Procedure: Upon employment, each workforce member privy to protected health information must sign off on our confidentiality agreement which covers HIPAA Security and sanctions.

Contractors must also sign off on our confidentiality agreement and our business associate agreement which clearly outlines the responsibilities of business associates to properly secure protected health information.

Staff members and contractors are also trained upon hire on the specific support systems used to assist clients with technical issues using our software.

HIPAA training will be conducted upon hire and on an annual basis using any of the following methods (which will be signed off by staff member and contractors):

- Outsourced onsite training

- Seminars
- Web based training, or
- In house training

Any training provided reinforces the individual responsibility aspect of securing electronic protected health information (EPHI) and on the common cyber security threats to EPHI (i.e. phishing and spoofing).

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Protection from Malicious Software*

Protection from Malicious Software		
Safeguard: Administrati	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(ii)(B)	Addressable

Requirement: Develop procedures for protecting our assets and confidential health information against malicious software.

Policy: We will guard against, detect, and report malicious software, including software that has not yet compromised the system but is suspect.

This includes firewalls, virus protection software, and other measures to protect the confidentiality, integrity, and availability of protected health information.

Procedure: Our databases are hosted within a cloud-based infrastructure which provides enterprise level firewalls as well as intrusion detection to secure our internal environment. In addition, the database(s) used to host protected health information or other sensitive data are encrypted at rest to protect against common crypto-virology attacks.

Based on risk, “free” versions of anti-virus are not to be used only robust enterprise level anti-virus (this applies to Microsoft operating systems due to higher risks).

Portable devices used by the business which ever store EPHI are encrypted using whole disk encryption or file/folder level encryption

consistent with our separate *Cryptology Policy on page 58 of this manual*.

The above also applies to any machines used by contractors to access private health information on behalf of our business.

Workforce members will report immediately any detected virus to the security official.

All staff members are required to sign our BYOD policy which outlines the requirements for personal devices used to access, transmit, or maintain electronic protected health information.

From an administrative standpoint, we also require all staff members be trained on common cyber security threats upon hire and annually.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Login Monitoring*

Login Monitoring		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(ii)(C)	Addressable

Requirement: Protect your assets and confidential health information by monitoring login attempts and reporting discrepancies.

Policy: Our system containing private health information will monitor failed login attempts.

Procedure: Any user logging into our cloud-based system containing electronic protected health information (EPHI) is proactively monitored by our system logging capability and the system will lock out user after no more than 3 failed login

attempts.

This is done to ensure our system is protected from “bot” operated “brute force” password hacking tools and/or denial of service style cyber threats.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Password Management*

Password Management		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(ii)(D)	Addressable

Requirement: Protect our assets and confidential health information by creating, changing, and safeguarding passwords.

Policy: Our business will create, change, and safeguard user IDs and passwords.

Procedures: Our alpha-numeric passwords will be compatible with those designed by our systems containing private health information (PHI).

Passwords will not relate to the user's personal identity, nor will two members of our staff have the same password.

Each workforce member and contractor is responsible for providing protection against loss or disclosure of any passwords in his or her possession. For example, passwords may not be posted on monitors or under keyboards or disclosed to other workforce members.

Passwords that are forgotten will not be reissued, but rather replaced.

Passwords for staff members may be initially assigned by the HIPAA security official but must be user selected upon first login.

User logins into the cloud based system containing private health information are monitored proactively by the logging abilities of the system.

Passwords will be revoked immediately when a workforce member

or contractor leaves employment.

Staff members and contractors are required to report any compromise of their password to the security official.

Passwords are not to be shared with other workforce members.

Based upon risk and per the National Institute of Standard and Technologies (NIST), all access from staff members (and contractors) into the backend or frontend of the system requires a password of at least 8 characters “complex” and (for backend access/frontend optional) an SSH key or a secondary pin (via smartphone) for two factor authentication.

NOTE: Two factor authentication may be optional for customer access – not required

This provides a two-tier level of access controls for the backend database access.

“Complex” meaning that an uppercase letter, lowercase letter, number, and a symbol must be used.

See BYOD policy for personal devices used by staff and contractors.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Incident Procedures

Implementation Specification: *Response and Reporting*

Security Incident Reporting		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(6)(ii)	Required

Requirement: Implement policies and procedures to address security incidents.

Policy: We will manage and mitigate the effects of suspected and known security incidents in the business.

Procedures: Our workforce members and contractors are responsible for reporting security incidents to the security official as soon as they are recognized.

Failure to report such incidents may result in sanctions, as appropriate.

Upon notification of a security incident, the security official will attempt to contain the incident and minimize damage to the business systems and data.

The security official shall document in a security incident report, the security incident and actions taken to minimize damage to the business computers.

The security official shall maintain a current written security incident log.

The security official shall determine the extent of reporting, including to outside authorities as appropriate, based on business and legal considerations, and in response to HITECH Act breach notification requirements.

The security official will review security safeguard procedures following any security incident, make appropriate changes to minimize recurrence of such incidents, discuss changes with

workforce members, and include these actions in the security incident report.

The Breach Notification Policy is also included within this booklet on page 49.

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Data Backup Plan*

Data Backup Plan		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(A)	Required

Requirement: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Policy: We will ensure our business has the ability to access private health information in the event normal access procedures are down.

Procedure: Our electronic protected health information (EPHI) is hosted within our offsite cloud-based location and is backed up daily and per service level agreement (SLA) by our cloud-based vendor but based on business needs.

The backups are done (on a daily basis) within the cloud-based environment which hosts our application using protocols which have been setup and defined by our business.

For disaster recovery purposes, the database containing the EPHI is replicated within multiple physical geographical locations within the cloud environment using point to point secured communications.

All backups go through data integrity checksums and will proactively notify the HIPAA Security Official or our vendor in terms of failure.

Vendor policies on Disaster Recovery can be ascertained by request.

NOTE: The information maintained within the business is not imperative to patient health and downtime can be absorbed

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Disaster Recovery Plan (Contingency Plan)*

Contingency Plan		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)	Required

Requirement: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence, such as fire, vandalism, system failure, or natural disaster, that damage systems containing electronic protected health information.

Policy: Our business will respond to emergencies that may impair the business's computer systems and electronic protected health information.

Procedures: Our organization understands the necessity of business continuity and disaster recovery.

A simple internet connection is all that is needed to securely access the systems containing the electronic protected health information (EPHI) in a secure encrypted manner.

This applies to the application side access (customer) as well as the backed access for our developers. The datacenter provides a service level agreement (SLA) regarding uptime.

The order of importance for our system is clearly understood by our HIPAA Security Official

Order of importance is:

1. DNS for IP address resolution
2. Internet Service Provider (must be up at the datacenter)
3. Gateway must be active
4. Application server hosting the system
5. Database server hosting the database

Vendor policies on Disaster Recovery can be ascertained upon request

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Emergency Mode Operation Plan*

Emergency Mode Operation Plan		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(C)	Required
Requirement: 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 the emergency mode. **Low Risk:** This is not a risk for our business. In this business model, accessing our systems containing electronic protected health information can only be done in a secure encrypted fashion (HTTPS SSL/SSH) regardless if in emergency mode or not by using a simple internet connection. There is no other way to access our systems which maintain the electronic protected health information unless via encrypted channels (both from front end as well as back end). The cloud vendor provides a service level agreement for uptime. NOTE: The information maintained within the business is not imperative to patient health and downtime can be absorbed		

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Testing and Revision Procedure*

Testing and Revision		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(D)	Addressable
Requirement: Implement procedures for periodic testing and revision of contingency plans. **Policy:** Our business will ensure data integrity is maintained by testing the database **Procedure:** Daily backups are confirmed for success or fail through data integrity checksums and a notification is proactively sent to our IT development team or HIPAA Security Official in the event of a failure. In this business model, a simple internet connection is all that is needed to securely access our 3rd party cloud environment (which hosts our systems) in a secure encrypted manner – this applies to our customer access (front end) as well as our developers on the (backend). The data maintained within the application is segregated by design.		

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Applications and Data Criticality Analysis*

Applications, Data Criticality Analysis		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(E)	Addressable

Requirements: Assess relative criticality of specific applications and data in support of other contingency plan components.

Policy: We have determined the applications and data that are most critical for operation of the business and have prioritized that to be internet access.

Procedures: Our business clearly understands the priorities in terms of data criticality.

An internet connection is all that our business requires to access our electronic medical records system (which contains electronic private health information) in a secure encrypted fashion.

As previously stated within our *Disaster Recovery Plan* policy on page 22, the order of importance for our system is clearly understood by our HIPAA Security Official.

Order of importance is:

1. DNS for IP address resolution
2. Internet Service Provider (must be up)
3. Gateway must be active
4. Application server hosting the system
5. Database server hosting the database

Vendor policies on Disaster Recovery can be ascertained upon request

HIPAA Security Rule: Administrative Safeguards

Standard: Evaluation

Implementation Specification: *Evaluation*

Evaluation		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Evaluation	68 Federal Register 8377 45 CFR 164.308 (a)(8)	Required

Requirement: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently in response to environmental or operational 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 security standards for the protection of electronic protected health information.

Policy: We will re-evaluate, through internal and external audits, all of our security policies and procedures at least every year to determine whether the risks can be reduced or efforts should be increased and new tasks assigned to a workforce member to manage.

Procedures: Our Security Official will:

- Utilize in-house auditing or outsourced audit services for a full "bird's eye view" of our businesses HIPAA HITECH Compliance.
- Evaluate risks at least every other year or whenever the business determines that risks or changes in its operating environment warrant review.
- Ensure staff members are trained for common cyber security threats as part of the overall HIPAA HITECH training which is conducted upon hire and annually.

HIPAA Security Rule: Administrative Safeguards

Standard: Business Associate Agreement

Implementation Specification: *Business Associate Agreement*

Business Associate Agreements		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Evaluation	68 Federal Register 8377 45 CFR 164.308 (b)(1)	Required
Requirement: In accordance with general rules of the security standards, a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf. This is permissible only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard such information in accordance with the standard for business associate contracts or other arrangements under organizational requirements. **Policy:** Our business associates may create, receive, maintain, or transmit electronic protected health information on our behalf only if the business obtains satisfactory assurances that the business associate will appropriately safeguard protected health information in accordance with the standard for business associate contracts. **Procedures:** In accordance with our policies and procedures, any entity deemed a business associate will be required to sign our business associates agreement accepting liability for any breach of ePHI or PHI. Our contractors are not only required to sign our business associates agreement but also sign off on our confidentiality/non-disclosure agreement. Our HIPAA Security Official or business owner takes responsibility of getting the agreements signed and saved digitally.		

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Contingency Operations*

Contingency Operations		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(i)	Addressable

Requirement: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data.

Low Risk: This is not a risk for our business.

In this business model, accessing our systems containing protected health information can only be done in a secure encrypted fashion regardless if in emergency mode or not.

There is no other way to access our systems which maintains the protected health information unless via encrypted channels both from front end as well as back end.

This is not deemed a risk due to the fact all of the electronic protected health information (EPHI) inside our applications and systems are within offsite 3rd party cloud location with redundant geographical backups and high levels of physical security meeting SOC2 level requirements.

Vendor policies on physical security can be ascertained upon request.

If ever applicable, any electronic protected health information downloaded to a local device is only done if the local device has whole disk encryption enabled – this applies to personal devices as well – this is consistent with our Cryptology Policy which begins on page 58 of this manual.

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Facility Security Plan*

Facility Security Plan		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(ii)	Addressable
Requirement: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. **Policy:** We will safeguard its facility and systems equipment from unauthorized physical tampering, and theft. **Procedures:** EPHI resides only within the secure offsite SOC2 level cloud environment per the sound policies of the vendor . Vendor policies on physical security can be ascertained upon request. There is no electronic protected health information (EPHI) in any form at the physical location of the business. All portable devices used by the business (including BYOD) which store EPHI are encrypted using whole disk encryption, this is to protect the information in the event of theft or loss of portable devices – this is consistent with our Cryptology Policy on page 58 of this manual.		

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Access Control and Validation Procedures*

Access Control and Validation Procedures		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(iii)	Addressable

Requirement: 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.

Policy: We will control and validate a person's access to our facility based on that person's role or function.

Procedures: As stated within our *Facility Security Plan* policy on page 29, EPHI resides only within the secure offsite SOC2 level cloud environment per the sound policies of the vendor. Vendor policies on physical security can be ascertained upon request.

There is no electronic protected health information (EPHI) in any form at the physical location of the business.

All portable devices used by the business (including BYOD) which store EPHI are encrypted using whole disk encryption, this is to protect the information in the event of theft or loss of portable devices – this is consistent with our Cryptology Policy on page 58 of this manual.

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Maintenance Records*

Maintenance Records		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(iv)	Addressable
Requirement: Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (e.g. hardware, walls, doors, and locks). **Not a risk:** Considering protected health information resides in an offsite (cloud-based) datacenter this is not deemed a risk to wrongful disclosure of electronic protected health information (EPHI).		

HIPAA Security Rule: Physical Safeguards

Standard: Workstation Use

Implementation Specification: *Workstation Use*

Workstation Use		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Workstation use	68 *Federal Register* 8378 45 CFR 164.310(b)(2)	Required

Requirement: 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 that can access electronic protected health information.

Policy: We have specified appropriate functions to be performed on each workstation in the facility or outside the facility, the manner in which they are to be used.

Procedures:

- Our security official shall be responsible for establishing and implementing workstation use procedures and physical access controls to servers which maintain protected health information – this is governed by the strict policies of our offsite 3rd party cloud-based datacenter which hosts our systems
- We shall comply with any software license agreements.
- Our business requires enterprise level antivirus and other protective software tools on each workstation and server.
- Machines are only to be used as needed for work purposes, no social media or any other sort of inappropriate web browsing is permitted while accessing systems containing protected health information.
- Where applicable, all staff are required to sign our BYOD and also our Telework policy

HIPAA Security Rule: Physical Safeguards

Standard: Workstation Security

Implementation Specification: *Workstation Security*

Workstation Security		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Workstation security	68 *Federal Register* 8378 45 CFR 164.310(c)	Required

Requirement: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Policy: We make sure that all workstations that access sensitive information are secure, restricting access to authorized users. Workforce members of our business are responsible for complying with our workstation security policy and related procedures.

Procedures: Our security official:

- Shall be responsible for and ensure access if appropriate for business associates

In addition:

- Enforces that workforce members shall not display written passwords on or near workstations, desktop surfaces, or in drawers, and shall not share passwords with other workforce members in the business.
- Shall take measures to shield electronic protected health information from unauthorized individuals.
- Based on risk, our staff member and contractor computers auto lock or drop to a password protected screen saver in no more than 30 minutes of idle time as a required local device policy.

See BYOD policy for personally owned devices.

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Disposal*

Disposal		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(i)	Required
Requirement: Implement policies and procedures to address the final disposal of electronic protected health information and the hardware or electronic media on which it is stored. **Policy:** We will delete or erase any electronic protected health information prior to final disposal of hardware or electronic media on which it is stored. Workforce members of our business are responsible for complying with our disposal policy and related procedures. **Procedures:** Our HIPAA Security Official or internal IT development group disposes of any old business owned media by logically wiping the drive using a utility meeting Department of Defense (DoD) standards or by use of physical destruction of the hard drive. All machines are maintained within physically secured areas prior to physical destruction or logical wiping. *See separate BYOD policy for personally owned devices*		

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Media Re-Use*

Media Reuse		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(ii)	Required

Requirement: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.

Policy: We will delete any electronic protected health information on electronic media although no media containing electronic protected health information (EPHI) resides at the facility.

Procedure: As a rule, no EPHI is maintained on local or portable devices within our business.

Nonetheless, when handing down computers within our business, the HIPAA Security Official or IT staff ensures that the device has the appropriate applications installed and that there is not any electronic protected health information (EPHI) on the device.

In addition, portable devices which maintain EPHI are encrypted using whole disk encryption consistent with our Cryptology Policy on page 58 of this manual.

See separate BYOD policy for personally owned devices

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Accountability*

Accountability		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(iii)	Addressable
Requirement: Maintain a record of the movements of hardware and electronic media and any person responsible therefore. **No Risk:** Based on the small size of this business this is not a perceived risk. However, this business maintains an asset list of business owned hardware which accesses, transmits, or stores EPHI To ensure no electronic protected health information (EPHI) is wrongfully disclosed due to theft or loss of device, we force all portable tablets and laptops to be encrypted if storing EPHI on the local device. Staff members who use personal devices are beholden to our BYOD and Telework policies.		

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Data Backup and Storage*

Data Backup and Storage		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(iv)	Addressable

Requirement: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Policy: Our business ensures that data backups are available in the event they are needed due to a physically mishap with a server

Procedure: As stated within our Data Backup Plan policy on page 21, our electronic protected health information (EPHI) is hosted within our offsite cloud-based location and is backed up daily and per service level agreement (SLA) by our cloud-based vendor but based on business needs.

The backups are done (on a daily basis) within the cloud-based environment which hosts our application using protocols which have been setup and defined by our business.

For disaster recovery purposes, the database containing the EPHI is replicated within multiple physical geographical locations within the cloud environment using point to point secured communications.

All backups go through data integrity checksums and will proactively notify the HIPAA Security Official or our vendor in terms of failure.

Vendor policies on Disaster Recovery can be ascertained by request

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Unique User Identification*

Unique User Identification		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(1)	Required

Requirement: Assign a unique name and/or number for identifying and tracking user identity.

Policy: Workforce members shall not share or otherwise disclose user IDs or passwords with any other individuals except for the three employees of the business.

Procedures: All internal staff and customers are assigned a unique user ID into any systems containing or accessing electronic protected health information (EPHI).

Customer user ID's are selected by the customer specific to their needs within their datasets.

Internal user ID's are manually assigned by the HIPAA Security Official or email address is used specific to the user

Passwords are not shared within the organization, this is forbidden for all internal staff and contractors

See separate BYOD policy which all staff members accessing protected health information are required to sign.

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Emergency Access Procedure*

Emergency Access Procedure		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(ii)	Required
Requirement: Establish and implement, as needed, procedures for obtaining necessary electronic protected health information during an emergency. **Low Risk:** This is not a risk for our business. In the business model, accessing our systems containing protected health information can only be done in a secure encrypted fashion regardless if in emergency mode or not. There is no other way to access our system which maintains the electronic protected health information unless via encrypted channels both from front end customer access as well as back end developer access.		

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Automatic Logoff*

Automatic Logoff		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(iii)	Addressable

Requirement: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Policy: Our security official shall make sure that automatic logoff procedures are in place on all systems and devices that provide access to sensitive information, including desktops, laptops, tablets, and handheld devices.

Procedures: Workforce members may frequently leave their workstations or laptops without time to completely log off the computer system.

The solution is to activate a password-protected screensaver or auto lock that locks a workstation or portable laptop and prevents unauthorized users from viewing or accessing sensitive information but that does not log the user off the system.

On the user's return to the machine, it is only necessary to reenter the password to gain access as before.

Password protected screen saver or auto lock is set to no more than 30 minutes for all machines accessing private health information, this is a forced local device policy within the organization.

For the application we provide to customers the auto-lock is based on customer preference.

See BYOD policy for personal devices.

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Encryption and Decryption*

Encryption and Decryption		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(iv)	Addressable

Requirement: Implement a mechanism to encrypt and decrypt electronic protected health information.

Policy: Our business will ensure that any electronic data being transmitted or physically taken offsite are to be secured.

Procedure: We ensure any electronic protected health information (EPHI) data in transmissions and at rest is secured by:

- Accessing our electronic protected health information (EPHI) system which is located within our cloud-based environment can only be done via secured encrypted channels regardless if accessing from the front end or the back end
- We ensure our database(s) hosting EPHI is physically secured at rest within our offsite datacenter behind multiple levels of physical and technological security measures meeting SOC2 level requirements
- Our database(s) maintaining the EPHI are encrypted at rest for added security against crypto-virology attacks and maintained behind layers of firewalls and technical security
- No private health information is ever emailed unless informational (i.e. *please login to system*) unless customer preference dictates otherwise
- No EPHI is ever transmitted or locally maintained on any portable devices unless encrypted using whole disk encryption

See Cryptology Policy beginning on page 58 of this manual

HIPAA Security Rule: Technical Safeguards

Standard: Audit Controls

Implementation Specification: *Audit Controls*

Audit Controls		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Audit controls	68 *Federal Register* 8378 45 CFR 164.312(b)	Required

Requirement: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Policy: Our security official or member of the IT staff must make sure that workforce members are in compliance with our technical safeguards pertaining to use of electronic systems and networks and access to and protection of electronic protected health information (ePHI).

Compliance means that use and access conform to the scope of each workforce member's responsibilities. The business shall take appropriate actions to correct inappropriate use or accessibility issues or incidents. The HIPAA Security Official must make sure that all existing and newly acquired software which is owned by the business and contains private health information has auditing capability, and that the auditing function is enabled.

Procedure: As stated within our Information System Activity Review policy on page 8, our HIPAA Security Official or designated member of the IT team is responsible for overseeing compliance of our policies and procedures by reviewing records of information system activity for inappropriate use on an "as needed" basis to ensure no inappropriate access is taking place within our systems which house the electronic protected health information (EPHI)

As needed a written account of audits is kept on within our *Access*

Monitoring Log (on page 53 of this manual) indicating when the audit was done, what was audited, and who conducted the audit.

Any of our staff members or contractors privy to private health information (or sensitive data) are subject to system use auditing to ensure access to patient information is appropriate.

System auditing is covered within any staff training given, and all staff members as well as contractors are aware of sanctions involving inappropriate access or snooping.

HIPAA Security Rule: Technical Safeguards

Standard: Integrity

Implementation Specification: *Integrity*

Integrity		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Integrity	68 *Federal Register* 8378 45 CFR 164.312(c)(1)	Required

Requirement: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Policy: We will ensure data is protected and secured.

Procedure: Our Security Official will ensure that our systems which maintain electronic protected health information (EPHI) maintain mechanisms that authenticate the integrity of confidential health information.

This is done by:

- encryption of portable tablets and laptops which maintain EPHI,
- unique user logins,
- use of the minimum necessary standard,
- system auditing enabled,
- high levels of physical security within cloud environment,
- file level encrypted application database at rest,
- end user tracking mechanisms,
- adequate staff training prior to accessing or entering live data into systems,
- and a complex password policy forced electronically by the system on the front end and back end

HIPAA Security Rule: Technical Safeguards

Standard: Integrity

Implementation Specification: *Mechanisms to authenticate ePHI*

Mechanism to Authenticate Electronic Protected Health Information		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Integrity	68 *Federal Register* 8378 45 CFR 164.312(c)(2)	Addressable

Requirement: Implement electronic controls to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Policy: Our business will ensure that private health information data be protected to a reasonable and appropriate extent. No private health information is ever to be sent or accessed by our business in a non-secure fashion.

Procedure: Based on risk, there are several areas where information may be damaged or altered, primarily due to human error, data input, or insufficient training. As a result, our organization will ensure that each user has access to system training to the extent needed to maintain the highest level of integrity.

This is to be done using a mentoring program upon employment which is part of mandatory training upon hire or contract.

Training is done specifically for the systems the staff member will be accessing and utilizing as part of their job function.

Additionally, access to systems containing electronic protected health information (ePHI) will be granted to users based upon the minimum necessary standard, which means users are only given the minimum amount of access needed to perform job function

and only based on approval of the HIPAA Security Official.

HIPAA Security Rule: Technical Safeguards

Standard: Person or Entity Authentication

Implementation Specification: *Person or Entity Authentication*

Person or Entity Authentication		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Person or entity authentication	68 *Federal Register* 8378 45 CFR 164.312(d)	Required

Requirement: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the person or entity claimed.

Policy: All of our machines that access private health information or the server that stores private health information will be password protected.

Procedures: Any workforce member or other person requiring access to sensitive information must provide verification that they are the person accessing the system using an assigned user ID and password.

Systems we access must require proof of identity that it can authenticate in one of three ways (we chose the first and the second):

- Something you know (e.g., user ID, mother's maiden name, personal ID number such as a national provider identifier, or password),
- Something you have (e.g., smart card, token, swipe card, or badge, SSH key), or
- Something you are (e.g., biometric such as a finger image, voice scan, iris or retina scan).

HIPAA Security Rule: Technical Safeguards

Standard: Transmission Security

Implementation Specification: *Integrity Controls*

Integrity Controls		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Transmission security	68 *Federal Register* 8378 45 CFR 164.312(e)(2)(i)	Addressable

Requirement: Implement security measures to guard against unauthorized access to electronic protected health information over an electronic communications network; ensure that electronically transmitted protected health information is not improperly modified without detection until disposed of.

Policy: Very low risk for use but we ensure that sensitive data is protected.

Procedure: Our security official or member of the IT staff will determine when, how, and if electronic protected health information (EPHI) will be shared over an electronic communications network.

Electronic protected health information will not be altered or destroyed in an unauthorized manner, that is, without knowledge or approval of our Security Official

Data integrity controls measure in place are:

- ensuring no EPHI is ever transmitted unless encrypted,
- unique assignment of user IDs,
- strong passwords of at least 8-characters with complexity,
- encrypted application databases which maintain EPHI at rest,
- encrypted channels for transmitting any EPHI,
- encryption of portable devices (which maintain any EPHI),
- and audit trails of user activity within the application and servers hosting our system

We will apply appropriate sanctions to the workforce member or contractors that made unauthorized changes and remind workforce members of the need to maintain integrity of electronic protected

health information.

HIPAA Security Rule: Technical Safeguards

Standard: Transmission Security

Implementation Specification: *Encryption*

Encryption		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Transmission security	68 *Federal Register* 8378 45 CFR 164.312(e)(2)(ii)	Addressable

Requirement: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Policy: Where reasonable we will ensure our business protects and encrypts private health information.

Procedure: We will ensure that any transmissions of electronic private health information (ePHI) be encrypted unless authorized to send in a non-encrypted manner.

This is done by use of secure encrypted remote access to and from our systems maintained within our offsite datacenter which contain electronic protected health information (EPHI), ensuring that no electronic protected health information ever is transmitted, stored, or physically taken offsite without encryption.

See Cryptology Policy beginning on page 58 of this manual

Breach Notification Policy

INTRODUCTION

A “breach” under the HIPAA Privacy Rule is an impermissible use or disclosure that compromises the security or privacy of unsecured protected health information (PHI) such that the use or disclosure poses a *significant* risk of financial, reputational, or other harm to the affected person(s). This does not include every impermissible use or disclosure.

UNSECURED PHI

Notification is required only if the breach involved “unsecured” protected health information. Unsecured protected health information (PHI) is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services.

Acceptable methods of securing PHI include the following:

- Encryption of data at rest that meets the National Institute of Standards and Technology (NIST) Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*
- Encryption for data in motion that complies with the Federal Information Processing Standards.
- Storage media has been destroyed in one of the following ways:
    - Paper, film, or other hard copy that has been shredded or destroyed in such a way that it cannot be read or reconstructed.
    - Electronic media that has been cleared, purged, or destroyed according to NIST Publication 800-88, *Guidelines for Media Sanitization,* so that information cannot be retrieved.

The Breach Notification Rule allows three exceptions:

- An *unintentional* acquisition, access, or use of the PHI by a member of the workforce acting under the authority of a covered entity or a business associate.
- An inadvertent disclosure of PHI by a person authorized to access the information to another person authorized to access the information *at the same covered entity or business associate*.
- The covered entity or business associate has a good faith belief that the unauthorized individual who received the information was *unable to retain the information*.

POLICY

In compliance with the Breach Notification Rule, we will make every effort to prevent breaches and to notify affected individuals as soon as possible after we discover a breach of unsecured protected health information. Notifications will comply as much as possible with all requirements included in the Breach Notification regulations.

As part of our periodic HIPAA training, every member of our workforce will be reminded of the responsibility to report breaches or suspected breaches. Training may be an in-house presentation, web casts, and written communications.

When a staff member becomes aware of a breach, he or she must notify the Privacy/Security Officer, who is responsible for investigating the incident, documenting all findings, and initiating notification processes required if the incident meets the above definition. This obligation is included in our periodic HIPAA training.

Copies of all documentation and notices will be maintained.

Any member of our workforce found violating this or any other HIPAA violation will be dealt with according to our HIPAA policy. A team of staff members will review each violation and will determine the course of action to be taken. Discipline to be implemented will be based on the seriousness of the violation and the number of violations committed by the individual.

INDIVIDUAL NOTICE: When a breach is discovered, we will notify each affected individual by first-class mail, or, if the individual has agreed, by e-mail. This notification will be done as quickly as feasible, within a maximum of sixty (60) days after the discovery of the breach.

If we have insufficient contact information for fewer than ten (10) affected by the information, we will use alternative means for contacting them, such as a telephone call or written notification to an alternate address provided by the individual. If we have insufficient contact information for ten (10) or more affected individuals, we will:

- Post the notification on our web site, or
- Provide notification in major print or broadcast media where the affective individuals likely reside.

The notification, regardless of mechanism, will include the following information:

- A description of the breach
- A description of the types of information involved in the breach
- Steps the affected individuals should take to protect themselves from potential harm
- What the business is doing to investigate the breach, mitigate the harm, and prevent further breaches
- Contact information for the business

For notices posted via print or broadcast media or on our web site, we will include a toll-free number for individuals to use to contact the business to determine if their information was included in the breach.

MEDIA NOTICE: If more than five hundred (500) individuals were affected by the breach, we will notify each individual as described above and will also provide notification to prominent media outlets serving the area where our patients reside. This will be in the form of a press release and will be provided within sixty (60) days of the discovery of the breach. It will include the same information used in the individual notice.

NOTICE TO THE SECRETARY: In addition to notifying individuals and, where necessary, the media, this business will notify the Secretary of the Department of Health and Human Services. This includes breaches affecting fewer than five hundred (500) individuals and will be done electronically through the HHS web site, using the form provided. For a breach that affects more than five hundred (500) individuals, this notification will be done within sixty (60) days. If the breach affects fewer than five hundred (500) individuals, the report(s) will be done annually, no later than sixty (60) days after the end of the calendar year in which the breach(es) occurred.

The web site is http://transparency.cit.nih.gov/breach/index.cfm. The form is entitled “Notice to the Secretary of HHS of Breach of Unsecured Protected Information.”

NOTIFICATION BY A BUSINESS ASSOCIATE: Our business associates are required to notify us if a breach of unsecured protected health information occurs at their business. This also must be done within sixty (60) days of discovery of the breach. They must provide a list of individuals affected and must provide information to allow us to notify our patients who have been affected. When we receive such information, we will immediately initiate our

notification process based on the number of individuals affected. The notification will include information used for other notifications.

OTHER CONCERNS: In addition to recognized breaches, we understand that some uses or disclosures may be perceived by some individuals to constitute a "breach." The individual who is concerned should contact our Privacy Officer, who will explain to the individual that such uses and/or disclosures do not constitute a breach. The Privacy Officer may reference our HIPAA Manual or (preferably) the HIPAA standards.

Breach Notification Template

Business Name: Zoom RPM

A security breach occurred at our business on (date) _____. Our initial investigation suggested that your protected health information may have been compromised.

Type of breach:
__ Theft __Loss __ Improper disposal __ Unauthorized access
__ Hacking/IT incident __Unknown __Other: _____

Location of breached information:
__ Business Associate __ Laptop __ Desktop computer __E-mail
__ Network server __ Other portable electronic device
__ Electronic medical record __ Paper __ Other: _____

Type of information involved in the breach:
__ Demographic information __ Clinical Information
__ Financial information __Other: _____

How the breach occurred:

_____

_____.

Safeguards in place prior to the breach:
__ Firewalls __ Packet filtering __ Secure browser sessions
__ Strong authentication __ Encrypted wireless
__ Physical controls __ Logical access controls __Anti-virus software
__ Intrusion detection __ Biometrics

To further protect your PHI, we recommend that you send a copy of this notice to
__Your bank and credit card companies and national credit bureaus (if financial information was involved)
__ Insurance company (if clinical information was involved)
__ Your Internet service provider (if e-mail information was included)

This business is currently conducting a thorough review to mitigate the situation and to prevent further breaches. We will inform you immediately if we discover additional information of use to you in this situation.

You may contact our Security Officer: Jonathan Cohen
By phone at:

Access Monitoring Log

Date	Data Monitored	Findings	Initials

Breach Incident Investigation

Date of potential breach:_____

Reported by: _____ Date: _____

1. What information was involved? _____

_____

2. What identifiers were included? _____

_____

3. What is the likelihood of re-identification? _____

4. Who received or used the information? _____

5. Was the PHI actually acquired or viewed? ____Yes ____No

6. What steps have been taken to mitigate the risk?_____

_____

_____

Conclusion:

____This incident was not a breach, so additional actions are not necessary.

____This incident was a breach, so Breach Notification is required.

Investigated by: _____ Date: _____

HIPAA Violation Summary Log

Number	Date of Discovery	Type of Violation	Resolution	Disciplinary Action	Date Completed
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

A security breach possibly occurred on (date) _____.

Type of breach:
__ Theft __Loss __ Improper disposal __ Unauthorized access
__ Hacking/IT incident __Unknown __ Other: _____

Location of breached information:
__ Business Associate __ Laptop __ Desktop computer __E-mail
__ Network server __ Other portable electronic device
__ Electronic medical record __ Paper __ Other: _____

Type of information involved in the breach:
__ Demographic information __ Clinical Information
__ Financial information __ Other: _____

How the breach occurred:

_____

_____.

PHI involved:

_____

_____.

Safeguards in place prior to the breach:

__ Firewalls __ Packet filtering __ Secure browser sessions
__ Strong authentication __ Encrypted wireless
__ Physical controls __ Logical access controls __Anti-virus software
__ Intrusion detection __ Biometrics

Additional information_____

_____

_____

Breach detected by: _____

Documented by: _____ Date: _____

Received by Security officer (date): _____

Termination Checklist

Employee Name: _____ Date: _____

- ☐ Exit interview (final day of employment)
- ☐ Computer system access blocked EMR/PMS (should coincide with exit interview)
- ☐ E-mail account forwarded to security officer
- ☐ Voice mail access eliminated
- ☐ All business-owned properties retrieved
- ☐ Key/badge/other access device returned to security officer
- ☐ Security access list updated to reflect termination
- ☐ Alarm system code changed if terminated individual had access
- ☐ Purchasing card, phone card, other company resources returned
- ☐ If terminated individual had purchasing authority, contact vendors to cancel employee from contract
- ☐ Terminated individual removed from company directory and listings
- ☐ Inform individual the date his/her 401K/medical/dental benefits will end
- ☐ Final time sheet submitted/final pay discussed
- ☐ Security notified of termination

_____ _____

Security Official's Signature Date

Cryptology Policy

Purpose and Scope

This policy governs the use of cryptology at Zoom RPM. All personnel of our organization are required to comply with this policy and demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Policy

Principles of Encryption

- Where possible all confidential and restricted information must be stored on a physically secured network server or within offsite datacenters with restricted access. Where it has been deemed necessary by senior management to store confidential information on any other than the Zoom RPM network servers or offsite datacenters used by Zoom RPM, the information must be encrypted.
- All confidential information maintained in drive shares or local databases must be encrypted where possible to mitigate the threat of crypto-virology attacks.
- All confidential information transmitted via email to an address outside the Domain, the information must be encrypted
- All passwords used as part of the process to encrypt/decrypt must be set to **at least** 8 characters and complex. "Complex" meaning the password must contain an uppercase letter, lowercase letter, number, and a symbol.

Servers in non-secured areas

- Confidential information stored on shared network servers or other computers which are situated in a physically non-secured location must be protected by strict access controls and encryption software.

Desktop Computers

- The desktop computers within our physical locations are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed. However, the following types of desktop computers will need to have encryption software installed.
    - Desktop computers which for business, geographic or technical reasons need to permanently store confidential information locally on the computer's hard drive (as opposed to a secure network server or secured offsite datacenter).
    - Desktop computers which for business, geographic or technical reasons need to permanently host information systems (for example, MS Access, Excel etc) that process confidential or restricted information locally on the computer's hard drive (as opposed to a secure network server or secured offsite datacenter).

- Desktop computers used by staff to work from home.
- Desktop computers which are located in unrestricted areas which are open to the public.
- Desktop computers which are located in third party facilities.

- The preferred method of encryption to be used is whole disk encryption

Laptops, Mobile Computer & Smart Devices

- All laptop computer devices must have IT approved encryption software installed prior to their use within network. In addition to encryption software the laptop must be password protected and have up to date anti-virus installed prior to their accessing or storing any confidential information.
- The mobile computer devices & smart devices must have device encryption enabled or approved encryption software installed prior to accessing or storing any confidential information.
- The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential information stored on the device.
- Laptop, mobile computer devices and smart devices MUST NOT be used for long-term storage of confidential information

Removable Storage Devices

- All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked area when not in use.
- The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential information stored on the removal storage device

USB Memory Sticks

- Confidential information may only be stored on approved encrypted USB memory sticks.
- IT approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential information. They MUST NOT be used for long term storage of confidential information.

- Confidential information stored on the approved USB memory stick MUST NOT be transferred to any internal (except a secure server or secured offsite datacenter) or external system in an unencrypted form.

Transmission Security

- All confidential information transmitted through email to an email address outside of the domain must be encrypted. The transfer of such information outside of the must be authorized by senior management. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

- Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via secure channels (for example: Secure FTP, TLS,
VPN etc). The transfer of such information outside of the domain must be authorized by senior management. The authorization must be issued in advance of the first instance and will apply thereafter if necessary.

- All confidential information transmitted around existing wireless networks must be encrypted using WEP (Wired Equivalent Privacy) or better. All new wireless networks installations must be encrypted using WPA (Wi-Fi Protected Access) or better.

Roles and Responsibilities

The HIPAA Security Official is responsible for:

- The selection and procurement of all encryption applications used within the organization

- The provisions, deployment and management of encryption applications within the organization

- The provision of training, advice and guidance on the use of encryption within the organization

- The implementation of this policy and making sure middle management of the organization clearly convey the policy to rank and file staff

- The ownership, management, control and security of the confidential electronic information processed by the organization

All staff members and users of IT resources are responsible for:

- Complying with the terms of this policy and all other relevant policies, procedures, regulations and applicable legislation

- Respecting and protecting the privacy and confidentiality of the information they process at all times.

- Ensuring all encryption passwords assigned to them are kept confidential at all times and not shared.

- Ensuring encryption passwords used to access encrypted devices are not written down on the encrypted device or stored with or near the encrypted device.

- Reporting all misuse and breaches of this policy to their manager

In addition to the above, the staff members' immediate supervisors are directly responsible for:

- The implementation of this policy and all other related to policies within the business areas for which they are responsible.

- Ensuring that all employees who report to them are made aware of and instructed to comply with this policy and all other relevant policies of the organization.

- Consulting with the human resources (HR) department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

Approved Encryption Algorithms and Protocols

- Symmetric Key Encryption Algorithms
    - Triple Data Encryption Standard (3DES) – minimum encryption key length of 168 bits
    - Advanced Encryption Standard (AES) – minimum encryption key length of 256 bits
    - Blowfish – minimum encryption key length of 256 bits

- Asymmetric Key Encryption Algorithms
    - Digital Signature Standard (DSS)
    - Rivest, Shamir, & Adelman (RSA)
    - Elliptic Curve Digital Signature Algorithm (ECDSA)

- Encryption Protocols

- IPSec (IP Security)
- SSL (Secure Socket Layer)
- SSH (Secure Shell)
- TLS (Transport Layer Security)
- S/MIME (Secure Multipurpose Internet Extension)

Enforcement

- Zoom RPM reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Zoom RPM staff members, contractors, sub-contractors who breach this policy may be subject to disciplinary action, including suspension, dismissal as well as civil and criminal charges.
- Breaches of this policy by a third party, may lead to the withdrawal of information technology resources to that third party or the Cancellation of any contract(s) between this organization and the third party.
- Zoom RPM will report any misuse of its IT resources to the appropriate authorities if deemed necessary

Review and Update

- This policy will be reviewed and updated on an “as needed” basis but no less than annually.

Definitions:

Asymmetric Key Encryption Algorithms: A class of encryption algorithm in which two different keys are used: one for encrypting the information, and one for decrypting the information (Public-key encryption)

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables our business to store sensitive information or transmit sensitive information across insecure networks (i.e. the internet) so that it cannot be read by anyone but the intended recipient

Confidential Information is the electronic information of a sensitive nature which is protected and maintained by our organization. The unauthorized access or accidental disclosure of this information could adversely impact our business, staff members of our business, business partners/contractors, and our clients. Some examples of confidential information include:

- Patient/client/staff personal data
- Patient/client/staff medical records
- Unpublished medical research
- Staff personal records
- Financial data
- Service plans / service performance monitoring reports
- Draft reports
- Audit reports
- Purchasing information
- Contract information of vendors
- Data covered by non-disclosure agreements
- Passwords/cryptographic private keys
- Data collected as part of HR investigations
- Incident reports

Encryption and Decryption Data that can be read and understood without any special measures is called “plaintext” or “cleartext”. The method of disguising plaintext in such a way as to hide its substance is called “encryption”. Encrypting plaintext results in unreadable gibberish called “ciphertext”. Encryption is used to ensure that information is hidden from anyone (or any entity) for whom it is not intended. The process of reverting ciphertext back to original plaintext is called decryption.

Zoom RPM Network: The data communications systems that interconnects the local area network (LAN) or remote cloud-based datacenters

Zoom RPM Server(s): Server(s) on the network or remote cloud-based datacenters which are used to manage or store sensitive data

Home Worker: Zoom RPM employee(s) who is authorized to work from their home (on a regular or occasional basis) instead of the organization’s facility.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smart phone devices (for example, Apple iPhones, Windows Mobile enabled devices, Google Android enabled devices, Nokia Symbian enabled devices, Blackberry RIM enabled devices etc). This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone

Personal information: Information relating to a living individual (employee, client and patient) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individual’s name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical

beliefs, trade union membership, political views, criminal convictions etc.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- •Obtaining, recording or keeping the information;
- •Collecting, organizing, storing, altering or adapting the information;
- •Retrieving, consulting or using the information;
- •Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- •Aligning, combining, blocking, erasing or destroying the information.

Removable storage Device:
Any optical or magnetic storage device or media including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external hard drives

Smart Device: A handheld mobile computer device which is capable of wireless connection (via WiFi, 3G, 4G etc), voice and video communication and, internet browsing etc. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc).

Symmetric Key Encryption Algorithms: A class of encryption algorithm in which the same key is used for both encryption and decryption of the information.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by Zoom RPM to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the business.

Transmission / Transmitted: The process of sending something (information or otherwise) from one location to another location.

Whole Disk Encryption: A method encryption where the entire contents (bits & bytes) of a magnetic or optical disk are encrypted