Managed Hosting

<COMPANY> Whitepaper on HIPAA Compliance

April, 2014

Table of Contents

Introduction

<COMPANY> is a secure managed hosting provider specializing in hosting security-sensitive customers with compliance requirements. Whether they be contractual or legal, we can help you with the security solutions you need. This whitepaper takes a look at a HIPAA compliant security program in a managed hosting environment.

If you are a Covered Entity (CE) per HIPAA or a Business Associate (BA) per 45 CFR § 160.103 you must be HIPAA compliant. This requires the implementation of a HIPAA compliant security program. Being that §164.502(e), §164.504(e), §164.532(d) and (e) and the HITECH Act specify that BAs must be HIPAA compliant just as CEs must, there is a good chance that your business must become HIPAA compliant. This requires the implementation of a HIPAA compliant security program including the appropriate security controls and documentation to protect electronic patient health information (ePHI).

This document was written to demonstrate what such a security program would look like and what it requires and should help to guide you in choosing and implementing an effective solution for HIPAA compliance in your managed hosting environment. A HIPAA compliant security program is a complicated and detailed undertaking. <COMPANY> has all of the skills and resources necessary to help your company implement a HIPAA security program.

The law effectively says to "implement the necessary safeguards." <COMPANY> can analyze your situation, perform a thorough risk assessment (required per HIPAA) and then select those necessary safeguards to mitigate the risks identified by the assessment.

<COMPANY> uses automated configuration management systems to reliably deploy extensive security controls and ensure they stay properly configured per the defined policy. Security controls are drawn from NIST SP-800-53, USGCB (US Government Configuration Baseline), NSA Hardening Guide, CIS benchmarks, among others.

<COMPANY> also implements a continuous monitoring approach to security which involves ongoing analysis of system logs and network traffic.

The law (45 CFR §160, 162, and 164) effectively says to "implement the necessary safeguards" and points to NIST SP-800-66 as the guidance in doing so. NIST SP-800-66 then goes on to point to other guidance, typically NIST ITL (National Institute of Standards and Technology Information Technology Library) publications. These are the standards that HIPAA compliant organizations are audited against by the US Department of Health and Human Services.

Full understanding and support from the highest levels of management are absolutely critical to the success of any security program. Every employee who will interact with the security program must understand the importance of security and adhering to policy.

The majority of software developers and system administrators are not accustomed to working in an environment containing federally regulated information such as ePHI. Security controls may chafe and annoy as developers have to adjust how they do things. It is imperative that company leadership support the security program and encourage employees to work within it.

For reference, the actual text of the HIPAA regulations from which most of the following is derived can be found at:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

Federal HIPAA Audit

The US Department of Health and Human Services Office for Civil Rights (US DHHS OCR) is responsible for HIPAA enforcement. This is the organization who would conduct an audit and enforce penalties if applicable.

There are three general ways to come to the attention of OCR and trigger an audit:

1. Have a security incident
2. Be chosen as one of their many random audits
3. Someone files a complaint

Note that if there is a security incident leading to ePHI compromise the BA or CE did not, by definition, "implement the necessary safeguards."

As required by section 13402(e)(4) of the HITECH Act, the “Secretary” (someone representing the DHHS) must post a list of breaches of unsecured protected health information affecting 500 or more individuals. Organizations who have a PHI data breach incident are publicly posted to the OCR "Wall of Shame":

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Such organizations may also appear among enforcement examples:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

And are then subjected to fines, audits, resolution agreement contracts, etc. In any event, the key to avoiding trouble and having a successful audit is to have faithfully fulfilled the requirements of HIPAA in both letter and spirit and to have good documentation to demonstrate compliance.

Compliance vs Security

All companies who have a compliance obligation must remember that the point of compliance is to impose a certain level of security. Security is the ultimate goal, not necessarily compliance. Compliance comes as a result of having a good security program. <COMPANY> will help you to avoid the "Checkbox security" mentality by ensuring effective security controls which not only meet the compliance requirements but provide practical and effective security measures to meet the actual need, not just the compliance need.

Being compliant does not mean you are secure. It merely means you have "checked the boxes". There are many things which could still result in a compromise such as an employee accidentally leaking his passphrase by getting his computer infected with malware, a bug in a web application exposed directly to the Internet, etc.

Occasionally it becomes necessary to go beyond the security requirements spelled out in the letter of the law. Compliance requirements should be considered "minimal acceptable practice" and not strictly "best practice".

Security is a process, not a product

Both compliance and security are ongoing efforts. There is no "We're HIPAA compliant, we're secure, we're done." There are always new vulnerabilities discovered, new versions of software coming out, and advances in the state of the art in terms of attacking and defending. The work is continuous and never-ending.

It has been said that compliance is not a checkmark, it is a culture. This is evidenced in companies who have successfully implemented a HIPAA compliant security program.

Prevention, Detection, Response

<COMPANY>'s security program has 3 main components: Prevention, detection, and response. Each of the security controls described herein can generally be classified as one of these.

Using secure passwords, keeping systems patched up, and even employee background checks (§164.308(a)(3)(ii)(b)) are considered prevention. These seek to avoid trouble in the first place.

But despite best efforts, since there is no such thing as 100% security, prevention cannot always be successful. We must also plan to detect problems such as intrusions or situations which could lead to intrusion and limit damage. Firewall egress rules, intrusion detection systems, and auditing/logging are all examples of critical methods of detection.

Finally, a plan must be in place to respond to an intrusion to prevent the situation from getting worse and to ultimately resolve the issue. This plan must be drafted taking the needs of the business into account. Responses involve, for example, isolating the trouble area, notifying the appropriate people, and taking proper remedial action.

Exposed web applications: Statistically the greatest weakness

The firewall is often seen as a primary security defense. And while it is certainly a necessary defense it is given far more credit to stop attacks than it deserves because the first thing anyone inevitably does after setting up the firewall is to open a hole in it to a sophisticated web application with lots of features and functionality which makes the web application a very large "attack surface" which can lead to security incidents.

Between SQL injections, path traversals, cross-site scripting, and many other attacks, web applications must be written very carefully and undergo thorough penetration testing and security review. Any application which has not yet had security review is practically guaranteed to have fatal flaws. This security review must be done on a recurring basis because added features and code changes can have a serious effect on the security of the application. If there were an SQL injection vulnerability (among

many other possible flaws) in the web app it would allow data to be stolen, deleted, or corrupted, possibly leaving no trace at all. The Client must ensure web application security.

Web application penetration testing is a necessity (§164.308(a)(8), NIST SP-800-66 4.8). It is not further discussed in this document but is a necessary part of HIPAA compliance for an organization offering a custom built web application on the Internet. <COMPANY> can help arrange for penetration testing to happen.

Keep in mind that when no vulnerabilities are found it does not mean there aren't any. All it takes is an attacker slightly more clever than whoever does the security testing to cause a serious problem.

While HIPAA security training is required for all staff having access to PHI (including outsourced staff, §164.308(a)(5)(i)), the Client is encouraged to seriously consider requiring security training for all developers.

Developers should, at the very least, be familiar with the OWASP Top 10: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf

HIPAA does not directly address web application security but the PCI-DSS (Payment Card Industry Data Security Standard) does and there is a standard for web developers to help ensure web app security (just replace card data, authorization data, etc. with PHI):

https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

Care should be taken to address application platform or programming language-specific issues. For example, if a web application is written in the extremely popular PHP programming language special attention should be paid to PHP-specific failures modes. Attention should also be paid to SQL injection which should be tested for extensively throughout the application. In <COMPANY>'s experience, every single proprietary PHP application of any significant complexity we have ever reviewed has had serious SQL injection flaws among other issues.

This report from Imperva outlines some of the more recent issues with PHP:

http://online.wsj.com/article/HUG1727897.djm.html

http://www.imperva.com/download.asp?id=421

Of course, Java, Ruby, Perl, Python, all have their issues which should be specifically addressed.

Application logging

While the Client's web application is out of scope for <COMPANY> services the following information is worth noting: HIPAA audit controls, mentioned in §164.312(b) apply to web application logging. Standard webserver logs are not sufficient. Application logs should say exactly what happened - when, where, how, and who. They should be intelligible without having the original software developer on hand. Every logged event should have a readable timestamp and every log related to user activity should contain the username of that user.

At a minimum the following types of information should be logged:

- Authentication decisions
- Health information access
- Health information adds, changes, deletions (both successes and failures)
- System changes

Passwords must never be logged and actual PHI must be kept out of logs. More discussion of application logging with respect to HIPAA can be found here:

http://www.markle.org/health/markle-common-framework/connecting-professionals/p7

DDOS, Disaster Recovery, Contingency Planning

While Distributed Denial of Service (DDOS) attack is a security issue (it affects the "availability" part of the Confidentiality, Integrity, Availability (CIA, §164.304) security triad) it is beyond <COMPANY>'s direct control. A best effort will be made to assist in such situations but results cannot be guaranteed. The client should make contingency plans to ensure the availability of the PHI per HIPAA under DDOS conditions if necessary. <COMPANY> can assist with the contingency planning process, business impact analysis and risk assessment, disaster recovery planning, etc.

Scope of services

The scope of services offered by <COMPANY> is necessarily limited to:

- The HIPAA "Security Rule" (45 CFR §160 and Subparts A and C of §164)
- Assets within <COMPANY> datacenter

Specifically excluded are:

- The Client's web application
- The Client's physical office premises and associated IT systems
- HIPAA electronic data interchange, transactions, identifiers, code sets
- HIPAA Privacy rule and any other aspects of HIPAA compliance

<COMPANY> can provide the technical security controls around the servers hosted in the <COMPANY> datacenter and assist with related documentation but complete HIPAA compliance requires much more including Client office premises security controls, employee training, documentation such as company security policy, among many other safeguards. This is all necessarily the responsibility of the Client.

Risk mitigation is the name of the game

There is no such thing as perfect or complete security. Each security control implemented is designed to reduce the probability of having an incident in some way. Sometimes it may seem that any one particular security control may not be terribly critical but remember that probabilities add up and anything that can be done to reduce the probably by even 1% can be worth it. To be able to mitigate risk an assessment must be done to identify the risk.

Risk Assessment

HIPAA requires that a risk assessment be performed in §164.308(a)(1)(ii)(A). Conducting a risk assessment is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Furthermore, periodic reviews and updates are required by §164.306(e) and §164.316(b)(2)(iii). For most clients, the risk assessment and all pertinent security documentation should be reviewed quarterly.

When thinking about risk, risk analysis, and mitigation business owners often ask themselves, "Why should we worry about security? Who would want to harm us? We are small and have nothing that would be useful or of value to anyone else." Aside from the threat of Federal enforcement action via civil and criminal penalties (sections 1176 and 1177 of the Social Security Act 42 U.S.C. 1320d–5, 1320d6) data is often valued for unexpected reasons:

- Data leakage - The personal details of individuals are of value to anyone planning identify theft, blackmail, etc.
- Extortion - Not only could individuals be extorted but the company itself could be extorted. There are numerous cases of databases being encrypted by attackers and the decryption password held for ransom. Or attackers could get in and then threaten to report the problem to DHHS OCR unless they are paid (which then, of course, becomes a never-ending extortion problem). On April 15th, 2014 the Harley Medical Group, a private cosmetic surgery firm in the UK, warned customers that attackers succesfully penetrated the company's computers and stole customer data in an extortion attempt. The breach affects 480 patients. The stolen data include names, addresses, email addresses, and procedures patients inquired about, but financial and medical records were not taken. The Harley Medical group has 21 clinics in the UK.

  http://www.v3.co.uk/v3-uk/news/2340171/hackers-hit-harley-medical-group-in-customer-data-extortion-attemp t

  http://www.telegraph.co.uk/technology/internet-security/10770922/Hackers-steal-500k-patient-records-from- Harley-Medical-Group.html

  Extortion demands are increasingly becoming part of online criminals' arsenals. Make sure to include this scenario as part of your incident response plans.
- Data deletion - Someone might want to take out a competitor.
- Defacement - If someone could modify the front page of the website it would cause reputational damage and affect customer confidence and possibly cause DHHS OCR involvement.
- Insiders - Ask a business owner, "How much is your data or 'intellectual property' really worth?" and you will likely be told a large sum. Then ask, "If someone offered just 1/10th that much to your average employee (knowing what they are paid in comparison) to put your data

on a USB drive and walk out with it, would they?" and the point is made. And that is just one of many possible motivations an insider may have.

Whether your organization is large or small it could have access to the ePHI of many patients consisting of gigabytes of data. You have a massive responsibility to protect that data worthy of a comprehensive security program. In the event of an OCR audit the size or means of the company is not considered. Compliance is not a function of the size of the organization. An organization is responsible for being compliant on each applicable requirement. It is not graded on a curve.

If your ePHI is somehow Internet-connected your organization faces the riskiest situation imaginable and OCR will expect significant measures to be taken to mitigate that risk.

The four essential steps to managing risk are:

1. Identify all foreseeable hazards that have potential to result in a breach of CIA.
2. Assess the amount of risk where:

   Risk = Threat * Vulnerability * Likelyhood * Impact
3. Control the risk or, if possible, remove the risk completely.
4. Review risk assessment to monitor and improve ‘control measures’

The scope of the risk assessment to be conducted by <COMPANY> is the physical servers and any virtual machines within them in the <COMPANY> datacenter and associated network connections and traffic. A semi-quantitative risk assessment approach as defined in NIST SP-800-30-Rev1 will be used.

Security Controls

A security control is anything which reduces risk. Each risk identified in the risk assessment must be addressed by a security control which is intended to reduce or mitigate that risk. The HIPAA law itself tends to be descriptive rather than prescriptive in how to implement the various security controls. It doesn't say exactly what to do and instead says things like "Protect against any reasonably anticipated threats or hazards" (45 CFR §164.306(a)(2)), for example. The general rule has been "if you had an intrusion, it wasn't protected against." at which point government action can be taken including fines etc.

The Security Rule of HIPAA requires organizations to “implement policies and procedures to prevent, detect, contain, and correct security violations.” (§164.308(a)(1)). Implementors of HIPAA compliant security programs are specifically pointed to published guidance for the more technical details of how to implement security controls. The National Institute for Standards and Technology (NIST), a US government standards organization, has developed a large body of technical guidance to be applied in situations such as HIPAA compliance. The US Department of Health and Human Services (the official central governmental hub for all HIPAA issues including rules, standards and implementation guides) specifically refers CEs and BAs to NIST SP-800-66 as primary guidance for implementing the "Security rule" which is the area of HIPAA legislation that concerns us for the managed hosting of the Client's ePHI.

The HIPAA Security Rule breaks down into three main areas which focus on maintaining the CIA of the ePHI:

- Administrative Safeguards

- Physical Safeguards
- Technical Safeguards

Most of this requires cooperation although some of it is entirely the Client's responsibility. For example, as noted above, Client's endpoints (workstations, mobile phones, etc.), physical facilities, employees, etc. are all beyond the scope of <COMPANY>'s responsibility. <COMPANY>'s responsibility shall be only the servers directly administered by <COMPANY> and the facility in which they reside.

Administrative Safeguards

- Privacy procedures and privacy officer: Client must have its own privacy procedures and a designated privacy officer. <COMPANY> has one for our part.
- Policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls: The Client must have executive sign-off on their own policies and procedures, and <COMPANY> shall have the same.
- Procedures clearly identify employees who should have access to PHI. Access to PHI must be restricted to only those employees who have a need for it to complete their job function: The Client must have this documentation as does <COMPANY>.
- <COMPANY> maintains an access list of who is allowed to make changes to the account and who is allowed to have access to the Client's server environment where the PHI is maintained.
- The procedures must address access authorization, establishment, modification, and termination: The Client must have this documentation as does <COMPANY>.
- Must have an ongoing training program regarding the handling of PHI provided to employees dealing with PHI: The Client must have such a program in place as must <COMPANY>.
- Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements: <COMPANY> does so, as does our datacenter physical security provider.
- A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place: <COMPANY> can provide documentation for backup procedures and can offer a disaster recovery site in a datacenter in another geographical region. The Client is responsible for their own contingency and disaster recovery plans and procedures for their other facilities not managed by <COMPANY>. Note that your information never leaves your servers except via your approved applications/methods and backups to our backup server which is on a separate VLAN not accessible to the Internet with strict access controls or encrypted off-site backup. Our own policy states that any disks that leave the facility which contained unencrypted customer information are securely wiped via documented procedure beforehand.
- Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations: <COMPANY> audits their own system security logs on a daily basis, a physical inspection of facilities once a quarter. In the event there is a security event additional audit procedures are performed appropriate to the event to ensure the integrity of the hosts, network, and associated infrastructure.

- Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations: <COMPANY> has such procedures.

Physical Safeguards

- Controls must govern the introduction and removal of hardware and software from the network: <COMPANY> logs all equipment as it physically enters and leaves the datacenter. When equipment is retired it is disposed of properly to ensure that PHI is not compromised including the secure wiping or physical destruction of media.
- Access to equipment containing health information should be carefully controlled and monitored: Both logical and physical accesses to the environment are logged and reviewed.
- Access to hardware and software must be limited to properly authorized individuals: <COMPANY> implements strict access controls via multiple levels of doors, locks (physical), and access control lists, cryptographic keys, and shared secrets (logical) among other mechanisms.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts: <COMPANY>'s datacenter provider has all of these things and logs all visitors, issues and requires badges be worn in the datacenter environment, etc.
- Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public: <COMPANY> implements these procedures and protects workstations used to access the data from unauthorized access.
- If the CEs or BAs utilize contractors or agents, they too must be fully trained on their physical access responsibilities: Other than <COMPANY>, only the datacenter facility provider has physical access and they are fully trained on their access responsibilities.

Technical Safeguards

Information systems housing ePHI must be protected from intrusion. In our HIPAA compliant hosting environment <COMPANY> implements many hardening measures to prevent and detect intrusion. This area is <COMPANY>'s greatest strength and value. It is also the largest and most complex area of security controls requiring exceptional skills to implement and maintain.

Linux Host Hardening

Our Linux host hardening program is based on the NSA Linux Hardening Guide also known as the NSA Systems Network Attack Center (SNAC) hardening guide:

http://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf

Chief among our hardening measures is the use of an automated configuration management system. This system automatically applies many config changes to a stock Linux server. It currently consists of over 3000 lines of code and covers automatic configuration and maintenance of security controls such as:

- File integrity monitoring (SNAC-2.1.3.1.1)
- System audit logs (file accesses, changes, etc) (SNAC-2.6.2.1)
- Secure automount configuration (SNAC-2.2.2.3)
- Disable avahi autoconf (SNAC-3.7.1.1)
- Configure warning banner (SNAC-2.3.7.1)
- Enforce secure bootup (SNAC-2.3.5.3)
- Enforce secure console permissions (SNAC-2.3.1.1)
- Disable coredumps to minimize chances of information leakage (SNAC-2.2.4.2)
- Disable atd, ensure proper cron file permissions (SNAC-3.4)
- Ensure execshield is enabled to thwart buffer overflow attempts (SNAC-2.2.4.3)
- Ensure proper mount permissions such as noexec etc. in fstab (SNAC-2.2.1.[1,2])
- Ensure proper home directory permissions (SNAC-2.3.4.2)
- Configure various kernel parameters, enable no-exec stack, disable hazardous drivers (SNAC-2.2.4.4.2)
- Ensure proper log rotation so as not to lose log data (SNAC-2.6.1.5)
- Disable certain esoteric kernel modules from loading, reducing attack surface (SNAC-2.2.2.5)
- Ensure NFS related services are disabled (SNAC-3.13.1.1)
- Enforce strong passwords, set lockouts, etc. (SNAC-2.3.3.1.1)
- Set password lockouts, hash algorithm, file permissions. (SNAC-2.2.3.1)
- Ensure root's $PATH is safe and sane (SNAC-2.3.4.1.[1,2])
- Configure postfix to not listen on network (SNAC-3.11.1.1)
- Regularly scan the system comparing rpm checksums with installed files (SNAC-2.1.3.2)
- Ensure sendmail is off and uninstalled (SNAC-3.11.1.1)
- Ensure a number of undesireable/unsafe services are disabled (SNAC-3.3.15.2)
- Set global umask settings (helps ensure safe file permissions) (SNAC-2.2.4.1)
- Disable wireless kernel modules (SNAC-2.5.2.2.3)
- Ensure proper SSH config, distribution of pubkeys, etc. (SNAC-3.5.2)

<COMPANY> also implements SELinux on all of our security hardened servers. This is a system of mandatory access controls (MACs) developed by the NSA:

http://selinuxproject.org

SELinux is indispensable in preventing security flaws in things such as web applications from accessing/changing other parts of the system as well as preventing many other classes of security problems.

<COMPANY> will configure SELinux to run in enforcing mode and confine processes to least

privilege to the greatest extent practical while still allowing normal operation.

Security patches will be applied within 30 days, Client permitting (reboots required).

Additional technical security controls:

- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner. <COMPANY> uses file integrity monitoring software plus audit system rules to track access and changes to files.
- Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity: <COMPANY> employs these technologies where appropriate.
- CEs and BAs must also authenticate entities with which they communicate: <COMPANY> has various ways to authenticate entities including public key cryptography, telephone callback, and token systems. SSH public key is the most commonly used method for system access. Other methods are available including GPG (for email) and Google Authenticator (system login) depending on the situation.
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance: <COMPANY> can provide such documentation to the government on request.
- Information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing: <COMPANY> employs version control software to manage the configuration of network devices and many other systems.
- Documented risk analysis and risk management programs are required: Risk management must include all aspects of the business therefore the Client is responsible for this portion of HIPAA compliance. <COMPANY> will cooperate in any reasonable way to facilitate and meet the needs of the Client's risk management program.

Xen hardening

As <COMPANY> has standardized on the Xen platform for virtualization, when virtualizaiton is used the hypervisor is hardened per the Xen CIS Benchmarks to the greatest extent possible:

http://benchmarks.cisecurity.org/tools2/xen/CIS_Benchmark_Xen_32_v1.0.pdf

As well as per NIST SP-800-125.

MySQL hardening

MySQL databases are hardened per the MySQL CIS Benchmarks wherever practical:

http://benchmarks.cisecurity.org/tools2/mysql/CIS_MySQL_Benchmark_v1.0.1.pdf

Encryption

When information flows over open networks encryption must be utilized: <COMPANY> uses SSH for administrative functions, GPG for email, and SSL for webserving of ePHI. The Client must do

similarly when interacting with <COMPANY> hosted services containing ePHI. Standard Linux whole disk encryption is also available although generally only recommended for mobile devices such as laptops.

<COMPANY> makes extensive use of SSH and SSH configurations to ensure confidentiality and integrity of data as well as requiring public key authentication for all external system access.

Network segmentation

The Client's environment will be maintained on its own private network separated from non-client systems via firewalls using VLANs. Web application servers, database servers, and development servers will all reside in their own separate VLANs and be protected from each other to the greatest extent practical.

Firewalls

Firewalls must be configured with both ingress and egress filtering per NIST SP-800-41. Most are familiar with the idea of firewalls blocking inbound connections but blocking unusual outbound connections is necessary also to prevent many kinds of attacks from working as well as exfiltration of data. Firewalls logging blocked outbound connections is an excellent source of information as to unusual things happening within the network.

The firewall blocks access to SSH on all of the internal servers. No direct connections can be allowed. An SSH bastion host with public key only authentication (effectively two-factor authentication when used with passworded private keys) is provided to facilitate SSH access to internal production servers. The bastion host will be hardened/locked down to the greatest extent practical.

As it is the only way to SSH into the environment special attention will be paid to SSH. Too many failed login attempts will cause the IP address of the user/attacker to be banned for a fixed amount of time to mitigate password guessing/brute force attacks.

Personnel who have never worked in a secured environment may be unfamiliar with the practice of using public key authentication, relaying their SSH connection through a bastion host, or not being able to make outgoing connections from the servers. These developers will require training. SSH, particularly the OpenSSH implementation, is not only the industry standard but is a very powerful tool for providing remote access and has facilities to make working among these restrictions easy.

Auditing

Regular analysis of system log files is an important means of detecting intrusions, intrusion attempts, software misconfigurations, among other things. It is critical to get the system log files off the server on which they are generated and onto a separate secured system where they cannot be tampered with.

System log files will be sent in real-time to a central log server where they can be subjected to weekly audit log reviews per §164.308(a)(1)(ii) (D) and NIST SP-800-66 section 4.1.7 .

The following regularly scheduled audits will be conducted:

- Weekly log file analysis
- Quarterly system audits to check for any unusual processes, accounts, etc.
- Quarterly physical security audits
- Quarterly internal and external vulnerability scans and remediations

Proof of audit log reviews, audits, findings, etc. will be retained for 6 years per §164.316(b)(2)(i).

Intrusion Detection Systems

NIST SP-800-53 calls for intrusion detection systems for information system monitoring, near real-time alerting of issues, etc.

One of the best ways to monitor network activity and detect network attacks is to use a Network Intrusion Detection System (NIDS). Such a system inspects all traffic going into and out of the network and applies rules and heuristics to network traffic to attempt to detect attacks and alert security personnel of potential issues. Data coming from the NIDS must be reviewed regularly and in a timely manner to ensure early detection of issues.

File Integrity Monitoring (FIM) is used to detect changed system files. This is automatically deployed by configuration management. Changed files are logged and appear in the periodic system log review.

The Linux audit system logs access to critical files and various important events and is automatically configured by Puppet.

Centralized logging aggregates all of this information and provides a platform in which to investigate issues and detect intrusions.

Netflow monitoring logs network traffic making it possible to detect unusual network traffic.

This combined IDS provides accountability for employees by tracking their network activity (§164.312 (a)(1)). It provides a quick clue regarding unauthorized host access for rapid response to PHI access, alteration and/or destruction (§164.312(c)(1) and §164.308(e)(1)) and detects malicious and suspicious network activity and works in conjunction with third party devices to mitigate or remediate security policy violations (§164.308(a)(1)(i)). IDS excels as an incident response tool and serves as a first responder technology that provides notification of potential issues.

Backups

All CEs, including medical practices and BAs, must securely back up "retrievable exact copies of electronic protected health information" (§164.308(7)(ii)(A)). The data must be recoverable such that you can fully restore any loss of data (§164.308(7)(ii)(B). <COMPANY> utilizes various methods to backup data depending on the kind of data. Data is sent to a secured backup server on a separate logical

network.

Backups must be tested. Backup is useless if the backed up data is damaged therefore the law requires that procedures for periodic testing and revision of contingency plans be implemented (§164.308(7)(ii)(D)). The Client must work with <COMPANY> to enable appropriate infrastructure to be in place to test backups including a dev/test environment and all appropriate tools and code to ensure that the backups are good.

Copies of backup data must be sent offsite for storage and protection (§164.308(a)(1)). <COMPANY> has an arrangement with a local secure record storage company to ensure that even if something happens to the datacenter building and server hardware the data will be preserved. <COMPANY> and the storage vendor have systems for tracking exactly where each backup volume is at all times. Backups are sent off site weekly.

Backups being sent off-site are encrypted with FIPS 140-2 Annex A compliant encryption (HITECH (Section 13402(h) of Title XIII HITECH Act, and §164.312(e)(1)(B)) with the encryption keys managed securely with a paper copy in a locked safe in a separate secure location. This takes the encrypted backups out of scope for HIPAA compliance so that in the unlikely event a hard drive is stolen or misplaced in transit there can be no breach.

Data must be backed up frequently (§164.308(a)(1)). Even daily full backups of frequently changing data are not sufficient. Frequently changed directories containing ePHI such as uploaded files and database contents such as transaction logs will be backed up every hour to a backup server.

Written procedures must exist related to the data backup and recovery plan (§164.312(b)(1) and §164.312(b)(2)(i)). <COMPANY> will produce these as they pertain to the system backups along with the other required compliance documentation.

Breach notification

The HIPAA Breach Notification Rule ("BNR") did not exist prior to the HITECH Act. Section 13402 of the HITECH Act requires a CE to provide notification to affected individuals and to the Secretary of HHS following a discovery of a breach of unsecured Protected Health Information. BAs are also required to notify the CE. <COMPANY> will notify Client of any breaches and it is Client's responsibility to do any further notifications.

Conclusion

HIPAA compliance is a complicated and ever-changing undertaking requiring specialized skills and technologies. As established throughout this document, HIPAA compliance involves many aspects of security including system hardening, auditing, monitoring, and documentation. Organizations that want

to avoid legal and financial exposure from failing to be HIPAA compliant must implement the required security controls and procedures internally or utilize a service that ensures all HIPAA requirements are met.

Compliance is a team effort and we look forward to working with you as you work towards HIPAA compliance.

Call <COMPANY> at 866-692-6745 to discuss your secure managed hosting and HIPAA requirements today!

