HIPAA Security Compliance and F5 Solutions

Overview

As more medical information, including patient records, are converted into electronic format and Internet usage continues to grow, healthcare organizations are finding themselves increasingly vulnerable to attacks. The complex challenge of securing information and maintaining strict levels of patient confidentiality is increasingly difficult since web based systems are widely used in order to provide easy and ubiquitous access to authorized users.

HIPAA, The Health Insurance Portability and Accountability Act, requires healthcare organizations to take added precautions to ensure the security of their networks and the privacy of patient data. This paper will provide an overview of HIPAA security compliance, explore how companies can mitigate their security risks and adapt a strong HIPAA compliant posture using F5 products, illustrate how F5 products map to specific HIPAA security rules, and explore some of the key reasons F5 products are unique in their ability to provide companies with a simple means to allow compliance with HIPAA.

Challenge

In today's economy, the normal work history of a typical employee at a single job is no longer 40 years and retirement. It is now typical to see employees change jobs every few years. With this in mind it is vital for employees to have health coverage between jobs. The original intent of HIPAA was to address this concern. The second issue HIPAA was designed to address was the wastefulness within the healthcare payment system. It was found in the US pre-HIPAA system, for every dollar spent on healthcare in the U.S., $0.62 is used for health coverage while $0.11 is consumed by fraud and $0.27 goes toward administration.

Accordingly, contained within HIPAA are five Titles:

I. Health Care Access, Portability and Renewability
II. Preventing Health Care Fraud and Abuse Administration Simplification: Medical Liability Reform
III. Tax Related Health Provisions
IV. Application and Enforcement of Group Health Plan Requirements
V. Revenue Offsets

All of the above Titles, except for #2, affect health insurance availability or insurability. Title #2 goes beyond health insurance, focusing on direction and guidelines for healthcare providers, insurers and/or payment clearinghouses. For example, Title #2 Part C, "Preventing Healthcare Fraud and Abuse," outlines 4 major points to consider when building technology compliant infrastructures for HIPAA. These four points are: Transactions, Identifiers, Privacy and Security (TIPS).

Think of TIPS as a pyramid where Security is the foundation and Transactions are the end goal. The base of this pyramid revolves around Security, implemented to ensure the integrity of all data. On top of Security is Privacy, which prevents the unauthorized dispersal of data. With Security and Privacy in place, Identifiers are useful for accurately routing data to the appropriate recipients. Finally, Transaction and Code Sets can be placed as the standardized means of presenting data.

Who Needs To Be HIPAA Compliant?

HIPAA compliancy applies to what's known as Covered Entities (CE). A CE is an individual or organization that falls into one of three groups: Health Plans, Healthcare Clearinghouses and Healthcare Providers. According to the US Department of Health and Human Services (HHS), the Administrative Simplification standards adopted by HHS under HIPAA applies to:

- A healthcare provider that conducts certain transactions in electronic form
- A healthcare clearing house (payment and reimbursement systems)
- A health plan (insurance)

Penalties For Non-HIPAA Compliance

According to the American Medical Association website, Covered Entities that are not in compliance face either civil or criminal penalties. Violations of the Administrative Simplification Regulations can result in civil monetary penalties of $100 per violation, up to $25,000 per year. As for criminal penalties, any person who knowingly obtains or discloses individually identifiable health information in violation of the Administrative Simplification Regulations faces a fine up to $50,000, as well as imprisonment for up to one year.

Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, and up to five years in prison. Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

HIPAA Security - Overview and Definition

The final rules derived from HIPAA's security requirements were published in the Federal Register on April 20, 2003. These rules went into effect on April 21, 2005 for Covered Entities except for Small Health Plans, which must comply by April 21, 2006. HIPAA's Security Rule is only applicable to Protected Health Information (PHI) this is created, maintained or transmitted electronically.

The HIPAA Security Rule defined four (4) general requirements:

- A CE must ensure the confidentiality, integrity and availability of all electronic PHI that it creates, receives, maintains or transmits
- A CE must protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- A CE must protect against any reasonably anticipated users or disclosures of such information that is not permitted or required under the privacy rule
- A CE must ensure compliance with the security rule by its workforce

The Security Rule contains standards and implementation specifications. A Standard specifies in general terms what a CE must do to be compliant; an Implementation describes how a CE may address the requirements.

Implementation Specifications

For HIPAA, Implementation Specifications are categorized as those that are required and those that are addressable.

- Required: Implementation Specifications that must be implemented by CEs as specified in the Security Rules.

- Addressable: The Implementation Specifications that CEs must assess as to whether each delivers a "reasonable and appropriate safeguard" in the CE's environment.

The decision about the reasonable and appropriate nature of an addressable specification rests on the CE and is based on its overall technical environment and security framework. This decision may rely on a variety of factors, including the results of risk analysis, measures already in place, and the cost of implementing new measures. Based on the results of this decision process, the CE may choose one of three options:

- Implement the specification
- Implement an alternative security measure to accomplish the purposes of the standard
- Not implement anything if the specification is not reasonable and appropriate AND the standard can still be met

Security Rules: Covered Domains

The Security Rules' Standards and Implementation Specifications covers five (5) domains:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Business Associate Contracts and Policies
- Procedure and Documentation

Administrative Safeguards - These focus on the IT security management process (the policies and procedures designed to identity, develop, implement and maintain security measures to protect PHI). In addition, the Administration Safeguards help to manage the conduct of the CE's workforce in actions that protect that PHI.

Physical Safeguards - Security measures that are designed to protect the CE's PHI and physical (building, routers, switches, servers, etc.) environment where it is located from natural disasters, environmental hazards and unauthorized intrusions.

Technical Safeguards - Technology related policies and procedures that safeguard the use and integrity of PHI.

Business Associate Contracts - Necessary to ensure that appropriate safeguards are in place for the CE's PHI and to individuals and organizations that must share the CE's PHI.

Policies, Procedures and Documentation - Ensures the CE's organization has formalized plans (policies, procedures and documentation) necessary to implement security.

Solution F5 Products and How They Match Up With HIPAA Security Rule Safeguards

The following is an overview of F5's solutions, followed by a matrix that shows how F5 products comply with the HIPAA framework and security rules.

TrafficShield

TrafficShield, a web application firewall, ensures the security of web-based applications which access or could be used to access patient records or other protected health information. This security must extend beyond encryption (which ensures privacy from outsiders) and authentication/authorization (which provide users access to a given application).

The HIPAA compliance exposure caused by web-based applications is that an authenticated, encrypted user (say, a customer checking his or her patient records) can tamper with the web browser to access other patients' records.

Given all the publicity around the vulnerabilities of web applications today, and the fact that 80% of enterprise hacking attempts happen through the web (Gartner), it is clear that a web application firewall is a necessary part of HIPAA compliance.

BIG-IP Application Traffic Management

The BIG-IP system combines high-performance hardware platforms with a powerful version of BIG-IP software (version 9) that incorporates advanced application traffic management and security features in a modular, full-proxy architecture. The foundation of the BIG-IP version 9 software is the Traffic Management Operating System (TM/OS) that allows the BIG-IP device to serve as a full proxy for traffic passing through it to and from the servers that sit behind it in the data center.

This capability allows the BIG-IP system to "understand" the content of applications and make decisions based on complex rules associated with a specific application. It differentiates the BIG-IP product from competing traffic management solutions which can recognize the nature of a message but can't understand it, just as an English speaker might recognize a conversation in Spanish or French without understanding what is being said.

By the same analogy, the BIG-IP device can understand what is being said, translate between the parties if necessary, and alter the content as needed to provide increased security and deliver functions that would otherwise require a change in the application itself.

FirePass SSL VPN

FirePass allows healthcare workers working from home or on the road secure remote access to network resources using any web-enabled device and over a range of access networks, regardless of location. With the FirePass platform, healthcare organizations benefit from superior performance and scalability, easy management, and the advanced application security. The product also offers the industry's only open Application Programming Interface (API), Visual Policy Editor and Software Developer's Kit (SDK), plus a host of unique features and capabilities.

Where F5 Products and HIPAA Adjoin Coverage

The following matrix focuses on the F5 product's relevance to the Physical, Technical and Administrative domains as found in the Security Rules' Standards and Implementation Specifications. The remaining two areas of Implementation Specification (Business Associate Contracts and Policies, Procedures and Documentation), while important, are not covered as F5 solutions do not provide additive value in these areas for achieving compliance.

Section of HIPAA Security Rule	NIST Special Publication 800-66[1]. Descriptions. HIPAA Safeguard R=Required / A=Addressable	F5 Solutions - HIPAA Framework
Administrative Safeguards		
164.308(a)(3)(i)	***Workforce Security:*** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	**The FirePass controller has:** -Granular user policy levels to accommodate the least privilege user access model -Extensive auditing and enforcement capabilities to implement procedures for Authorization and Supervision

164.308(a)(3)(ii)(A)	***Authorization and/or Supervision (A):*** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	**The FirePass controller has:** -Granular user policy levels to accommodate the least privilege user access model -Extensive auditing and enforcement capabilities to implement procedures for Authorization and Supervision
164.308(a)(3)(ii)(B)	***Workforce Clearance Procedure (A):*** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	
164.308(a)(3)(ii)(C)	***Termination Procedure (A):*** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	
164.308(a)(4)(i)	***Information Access Management:*** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements.	**The FirePass controller**: -Helps to ensure the policies for Information Access Management are enforced. -Helps to ensure the policies and procedures for protecting EPHI within the clearinghouse. -Allows for granular control to applications and services based on the role/group/trust-level of user and device, thereby helping to ensure authorized access based on the policies and procedures. -Allows for a central control point of access establishment and modification. This will help ease the burden of management and consolidate the number of devices needed to deliver secure and trusted access that meets or exceeds the established policies and procedures.
164.308(a)(4)(ii)(A)	***Isolating Health Care Clearinghouse Functions (R):*** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	
164.308(a)(4)(ii)(B)	***Access Authorization (A):*** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	
164.308(a)(4)(ii)(C)	***Access Establishment and Modification (A):*** Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	

164.308(a)(5)(i)	***Security Awareness and Training (R):*** Implement a security awareness and training program for all members of its workforce (including management).	**The FirePass controller**: -Places regular security reminders on the login. -Helps to ensure that devices requesting access meet certain levels of trust in order to gain access to EPHI. -Provides extensive host checking capabilities (Over 100 checks including most Anti-Virus, Personal Firewalls, Google Desktop Search, Processes, Registry Settings, Files, OS and Browser Patch Levels). -Provides customization of the webtop that could give instructions log-in/log-off the system and proper password procedures. -Provides customization of the FirePass webtop that could give instructions on how to select the proper passwords and how to remember them.
164.308(a)(5)(ii)(A)	***Security Reminders (A):*** Periodic security updates.	
164.308(a)(5)(ii)(B)	***Protection from Malicious Software (A):*** Procedures for guarding against, detecting, and reporting malicious software.	
164.308(a)(5)(ii)(C)	***Log-in Monitoring (A):*** Procedures for monitoring log-in attempts and reporting discrepancies.	
164.308(a)(5)(ii)(D)	***Password Management (A):*** Procedures for creating, changing, and safeguarding passwords.	
164.308(a)(6)(i)	***Security Incident Procedures (R):*** Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii)	***Response and Reporting (R):*** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	**FirePass provides:** -Customization of the FirePass webtop which can give instructions on who to call if a suspected security incident occurs. -Extensive capabilities to direct user sessions to lesser privileged sessions if an incident is suspected.
164.308(a)(7)(i)	***Contingency Plan (R):*** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	BIG-IP Global Traffic Manager (GTM - formerly 3-DNS) has the capability to direct users to another data center if there is an outage at the active data center.
164.308(a)(7)(ii)(A)	***Data Backup Plan (R):*** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	

164.308(a)(7)(ii)(B)	***Disaster Recovery Plan (R):*** Establish (and implement as needed) procedures to restore any loss of data.	BIG-IP Global Traffic Manager (GTM - formerly 3-DNS) has the capability to direct users to another data center if there is an outage at the active data center.
164.308(a)(7)(ii)(C)	***Emergency Mode Operation Plan (R):*** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	
164.308(a)(7)(ii)(D)	***Testing and Revision Procedure (A):*** Implement procedures for periodic testing and revision of contingency plans.	
164.308(a)(7)(ii)(E)	***Applications and Data Criticality Analysis (A):*** Assess the relative criticality of specific applications and data in support of other contingency plan components.	
Physical Safeguards		
164.310(c)	***Workstation Security (R):*** Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.	FirePass is often used to validate trust levels with Users and Workstations.
Technical Safeguards		
164.312(a)(1)	***Access Control (R):*** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	FirePass has the ability to enforce granular policies based on trust levels established with the User and their Device. Based upon the Trust level FirePass can grant access to the appropriate resource containing EPHI.
164.312(a)(2)(i)	***Unique User Identification (R):*** Assign a unique name and/or number for identifying and tracking user identity.	Both FirePass and BIG-IP can integrate with various Directory Services such as LDAP, RADIUS, Active Directory, SSO and others.
164.312(a)(2)(ii)	***Emergency Access Procedure (R):*** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Because the FirePass provides access via a browser and SSL, an administrator should be able to access their environment from any location at any time.
164.312(a)(2)(iii)	***Automatic Logoff (A):*** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	FirePass will automatically logoff users due to inactivity. This can be configured by the administrator.

164.312(a)(2)(iv)	***Encryption and Decryption (A):*** Implement a mechanism to encrypt and decrypt electronic protected health information.	FirePass, BIG-IP and TrafficShield can participate in the offloading of SSL from web servers. All F5 platforms have high-end SSL termination hardware included.
164.312(b)	***Audit Controls (R):*** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronically protected health information.	All F5 solutions have extensive logging capabilities allowing for compliance-level auditing.
164.312(c)(1)	***Integrity (R):*** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	FirePass has the ability to validate checksums on files located on the remote devices. Checksum can be validated via MD5 & SHA-1 Hash for example.
164.312(c)(2)	***Mechanism to Authenticate Electronic Protected Health Information (A):*** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	FirePass has the ability to validate checksums on files located on the remote devices. Checksum can be validated via MD5 & SHA-1 Hash for example.
164.312(d)	***Person or Entity Authentication (R):*** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Both FirePass and BIG-IP can integrate with various Directory Services like LDAP, RADIUS, Active Directory, SSO, NT Domain, Client Certs & others.
164.312(e)(1)	***Transmission Security (R):*** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	BIG-IP, FirePass and TrafficShield can enforce the SSL key length used, such as 128 bit. In addition, these solutions have the ability to implement SSL certificate security via FIPS 140-2.
164.312(e)(2)(i)	***Integrity Controls (A):*** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	FirePass has the ability generate and distribute x.509 client certificates. In addition, FirePass can revoke the certificate based on any attribute within the certificate.
164.312(e)(2)(ii)	***Encryption (A):*** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	BIG-IP, FirePass and TrafficShield can enforce the SSL key length used, such as 128 bit. In addition, these solutions have the ability to implement SSL certificate security via FIPS 140-2.

[1]NIST Special Publication 800-66 "An Introductory Guide for Implementing the HIPAA Security Rule" http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf

About F5 F5 enables organizations to successfully deliver business-critical applications and gives them the greatest level of agility to stay ahead of growing business demands. As the pioneer and global leader in Application Traffic Management, F5 continues to lead the industry by driving more intelligence into the network to deliver advanced application agility. F5 products ensure the secure and optimized delivery of applications to any user - anywhere. Through its flexible and cohesive architecture, F5 delivers unmatched value by dramatically improving the way organizations serve their employees, customers and constituents, while lowering operational costs. Over 9,000 organizations and service providers worldwide trust F5 to keep their businesses running. The company is headquartered in Seattle, Washington with offices worldwide. For more information go to www.f5.com.