



www.oceanasensor.com

HIPAA and Data Security White Paper

Healthcare Insurance Portability and Accountability Act (HIPAA) regulations and consumer demand for protection of healthcare information have made the control of access to personal information a top concern among healthcare professionals. HIPAA, provides a set of instructions and guidelines for the encoding, privacy, security, integrity, and availability of patient health data. These guidelines require security and encryption for four types of private and protected health information: "data in use", "data in motion", "data at rest", and "data disposed".

HIPAA applies to any organization that transmits any electronic billing information (such as invoices, or information needed to look up insurance information) to any health insurance company, including Medicare or Medicaid. This means that HIPAA typically regulates organizations involved in health care, including organizations providing counseling, therapy, or other services that need to bill insurance companies. If a company bills or conducts any billing-related electronic communications with insurance companies, no matter how minimal, the entire organization is a "covered entity." This means that all data, processes, and systems throughout the organization are subject to the HIPAA guidelines.

This year marks 14 years since the passage of HIPAA. Apart from the colorful new terms to express frustration, HIPAA compliance is a process, not a destination, of implementing a strategy for secure access to personal healthcare records that addresses current regulations and scales to accommodate new ones. Noncompliance—in addition to being a legal headache and a disservice to patients—costs healthcare organizations time and money. A way to secure access to healthcare data and infrastructure providing the highest degree of protection while minimizing IT costs is needed, enabling new levels of business agility and improving employee productivity.

Originally, HIPAA called for civil and criminal penalties for privacy and security violations, including: fines up to \$25K for multiple violations of the same standard in a calendar year - fines up to \$250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information. In 2009, the federal government through the Health Information Technology for Economic and Clinical Health (HITECH) Act increased the maximum penalty to \$1.5 million for violations of rules under HIPAA. These HITECH Act revisions also encourage prompt corrective action and new security measures. Additionally, measures will soon be in place that allow for individual legal action related to personal information security breaches.

So where do security breaches occur? According to the Gartner Group in industry in general, 84% of high-cost security incidents occur when insiders release confidential data. Also, in the U.S., the FBI estimates that 70% of all security breaches come from inside the organization when data is stored on networks in database and inside firewalls. Internal intrusion and data

access needs to be addressed in order to thwart the majority of these breaches. The Healthcare industry is not immune to these statistics. The following are some examples of HIPAA violations that have occurred.

Example 1: *What began as routine file maintenance, ended in arrest and possible jail time for a licensed practical nurse who shared a patient's medical information with her spouse.*

Ms. A, 29, had been employed by a midsize regional clinic for five years. While she enjoyed her job and got on well with her supervisor, Dr. P, she was known to bemoan what she saw as low pay and the financial strain it created for herself and her husband. That strain intensified when her husband was in an auto accident and then sued by people in the other car seeking compensation for their injuries. One day, as Ms. A was flipping through charts to straighten up the files, she saw the plaintiff's name. Reading the chart with great interest, she jotted some notes, stuck them in her bag, and replaced the file. That night, as her husband complained about the impending lawsuit and its potential financial consequences, Ms. A smiled and reached into her bag for the notes she had taken earlier. "I think this will help." she said.¹

Example 2: *Connecticut Attorney General Richard Blumenthal has filed a lawsuit charging Health Net of Connecticut Inc. with violations of the HIPAA privacy and security rules following a large breach of identifiable medical records and Social Security numbers. Blumenthal's office believes this is the first lawsuit by a state's chief legal officer since the HITECH Act last year gave state attorneys general authority to prosecute HIPAA privacy and security violations. Parent company Health Net in Los Angeles last November reported to insurance officials in four states the disappearance in May of protected health information on 1.5 million members, including 446,000 in Connecticut. The data was not encrypted, but Health Net said it is not visible without the use of specific software.²*

Example 3: *Houston, Texas: Sixteen hospital employees were fired for accessing the medical record of a medical resident who was hospitalized after being shot during an attempted robbery. According to George Hulme's blog for Health Information Trust Alliance, this looks like a simple case of hospital employees "snooping" to find out confidential patient information. The employees who accessed the data were in both clinical and administrative roles. Another thing to think about: How was the hospital able to identify the people who viewed her record? Hulme hypothesizes that the hospital was monitoring and logging patient record access and was alerted to the increased interest in this patient's medical record.³*

These are only a few of thousands of examples of violations in the Healthcare industry. Certainly most health care employees understand the HIPAA rules and receive compliance training. The organizations contract for HIPAA consulting to deliver this training at great expense to the industry. However, violations are on the rise and certifications are in jeopardy. The most important issue after all that training etc. is that most intrusion violations are identified after the fact. In each of the examples above the data was breached and the damage was done. There is a significant need for a proactive effort to stop employees before there is a HIPAA violation and more importantly before sensitive data is distributed erroneously or maliciously.

¹ <http://www.renalndurologynews.com/staff-nurse-faces-jail-time-for-hipaa-violations/article/119854/>

² <http://www.healthdatamanagement.com/news/breach-hipaa-privacy-security-hitech-lawsuit-39645-1.html>

³ <http://www.livingstonbuzz.com/2010/01/07/a-tale-of-two-hipaa-violations/>

The risk becomes greater as the nation implements more electronic medical records and Healthcare Data Interchanges.

HIPAA privacy regulations require that the use of personal health information be limited to that which is minimally necessary to administer treatment. The Act specifies that each employee throughout the entire organization should only see the "minimum necessary" information to do his or her job. Frequent changes in who is allowed access to personal information multiply the already complex task of access control. Everyday business events such as employee turnover, emergency access, promotions, job rotations, and changes in agreements with business partners, all require the associated changes in the access control mechanisms. Many of the personnel who utilize this information change frequently, while other accounts are temporary or require increased level of access for a short amount of time. This dynamic nature of accounts, privileges, and access levels makes the task of account provisioning, maintenance, and termination one of the most difficult tasks in the secure operation of HIPAA compliant information systems. The key to access control is to have an intuitive system that allows managing this complex task quickly and efficiently.

There is a ready-made solution for this industry that will protect data from access by employees and others who do not have the appropriate credentials and the need to know. Real time protection of data can be accomplished today with security middleware tools. Fortress Secure Interface™ is the solution that is well suited for requirements of HIPAA and broader-based Joint Commission (JCAHO) certifications. Specifically, it is the Fortress Secure Interface® -a cross-platform, rules-based, very-low-overhead, data field-level security middleware that manages both dynamic data security (data in flight) and static data security (data at rest). Generally, the FSI™ system was designed with the following attributes:

- State of the art security functionality that is easy to use and addresses the Healthcare industry's need to protect patient information, personnel data, electronic medical records and business process logic to name a few.
- A rules engine that is easy to use, provides real time alerts, a security audit trail and blanks out data elements on user's application screens based on their individual roles.
- The organization's current HIPAA policies and procedures are easily translated, administered and implemented by the rules engine.
- An architecture that supports the protection of dynamic and static data sources in real-time.
- A secure interface between internal clients, external clients and business partners to proprietary or sensitive application data as required by HIPAA.
- A secure application that is FIPS 140-2 certified by the federal government.
- Scalable solutions that can accommodate any number of data sources, terabytes of data and thousands of users.
- Affordable for a rural doctor's office or the entire national healthcare system.
- A rapidly deployed enterprise solution that takes days to implement not months.
- Integrates with a wide range of applications, databases and software tools.

In the examples above the Fortress Secure Interface® system's impact would have saved dollars but more importantly eliminated HIPAA violations and security breaches. The occurrence in Example 1 was theft of information from a paper records. Its' purpose is to focus attention on

1632 CORPORATE LANDING PARKWAY • VIRGINIA BEACH, VA. • 23454

PHONE: 757-426-3678 • FAX: 757-426-3633

Richard W Lally
CEO / President
rlally@oceanasensor.com
Type text]

Louis C Dommer III
COO / Sr. Vice President
ldommer@oceanasensor.com

the importance of securing medical records as more become mandated Electronic Health Records (EHR). The combination of EHRs and FSI's capability would have blocked access to this record and have alerted the hospital of the intrusion. Example 2 clearly would have been mitigated by FSI. The rules established by FSI would have denied access to the database. It would have also controlled through its rules engine data elements such as social security number, patient name/address and diagnosis to name a few that should never be downloaded by any employee. FSI is designed to control "snooping" as indicated in Example 3. Based on employee identity and role the organization's rules are inserted in the system. FSI would have limited access to the record as well as data elements within it. The culprits would have been caught by the alert function but data would never have been breached.

In summary, HIPAA and EHRs are the standard that Healthcare must follow. Utilizing an available security middleware, Fortress Secure Interface enables healthcare organizations to leverage the benefits of a dynamic and static data security tool to achieve the standard. This tool reduces potential HIPAA violations by automating security decision making while reducing security management costs. Implementation of its capabilities provides the organization's employees, clinicians, business associates and others with only the data they need to perform their job or task. Thus, the elimination and exposure to information breaches and potentially detrimental violations becomes a manageable task.

When faced with the potential liability for violations of the HITECH Act, the Fortress Security Interface is a cost effective solution to data security.

1632 CORPORATE LANDING PARKWAY • VIRGINIA BEACH, VA. • 23454

PHONE: 757-426-3678 • FAX: 757-426-3633

Richard W Lally
CEO / President
rlally@oceanasensor.com
Type text]

Louis C Dommer III
COO / Sr. Vice President
ldommer@oceanasensor.com