FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

4 Steps to Implementing Data Protection in Healthcare

A Best Practices Framework

1. A. Understand – HIPAA/HITECH Regulatory Lesgislation

The need to protect individual patient medical records has become well-established since the U.S. Government Health Information Portability and Accountability Act, HIPAA, was enacted in 1997 to define and enforce nationwide standards for such protection. The Health Information Technology for Economic and Clinical Health, HITECH, Act was signed into law in 2009 as a companion to HIPAA to, in particular, stimulate the adoption of Electronic Health Records and supporting technology. Since then these have collectively become known as the HIPAA/HITECH requirements. More recently the U.S. Department of Health and Human Services (HHS) has issued its Omnibus Ruling of 2013 that further clarified many of the earlier requirements and described a more active vigilance in monitoring compliance.

Personal, Private, or Protected Health Information (PHI) generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a healthcare care professional to identify an individual and determine appropriate care. These and other details are described in a set of "Rules":

- **Privacy Rule**
  A summary of key elements including who is covered, what information is protected, and how protected health information can be used and disclosed may be found on the HHS web site www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.
- **Security Rule**
  Establishes standards to protect individuals' electronic personal health information that is created, received, used, or maintained by requiring appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Reference: 45 CFR Part 160 and Subparts A and C of Part 164.
- **Enforcement Rule**
  Contains provisions relating to compliance and investigation, the imposition of penalties for violations, and procedures for hearings. Reference: 45 CFR Part 160, Subparts C, D, and E.
- **Breach Notification Rule**
  Issued in August, 2009, to implement section 13402 of the HITECH Act by requiring notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.
- **Omnibus Rule**
  Issued in January, 2013, to clarify these rules and to provide improved guidance for their execution and enforcement. An overview of the Omnibus impact may be found in the Code Green Networks white paper: "HIPAA Omnibus Compliance" at https://www.codegreennetworks.com/resources/downloads/HIPAAOmnibus.pdf.
- Enforcement of the Omnibus Rule began in September, 2013, which puts added incentive and urgency to all handlers of Personal Health Information to review their policies and procedures.
- The Omnibus rule clarifies the regulations to mean that any party who "creates, receives, maintains or transmits Personal Health Information" is covered under the same HIPAA//HITECH provisions. Business Associates and their subcontractors are, therefore, now subject to HIPAA/HITECH compliance requirements and potential audits as well.
- Certain individual states may have regulations in addition to the national standards mentioned above. Moreover, a particular enterprise could have additional governmental or industry compliance requirements that can be addressed by the application of a DLP solution. For instance, many health care companies may need to meet requirements defined by the Payment Card Industry (PCI). However, to maintain the stated focus of this paper, these regulatory requirements will not be addressed in detail here.

1. B. Understand - Compliance and Risks

The improper release of regulated health information can result in painful consequences to the organization(s) responsible - ranging from damaging media exposure

to harsh fines of up to $1,5m for serious incidents. Maintaining compliance with government regulatory acts to protect patients' private medical information needs to be a top issue for healthcare organizations and their business associates holding this type of information.

A proper Data Loss Prevention, DLP, technology when implemented appropriately will help address these requirements and reduce the risks involved.

1. C. Understand - What is DLP?

Data Loss Prevention, DLP, refers to technology employed for the purpose of reducing the risks from loss of control over sensitive data. Not all DLP offerings on the market are equal, however. Because of its unique advantages and powerful capabilities, DLP, here, will be taken to mean "Content Aware DLP" which is often referred to as "Enterprise DLP". Gartner, Inc. provides this definition in its IT Glossary:

> "Content-aware data loss prevention (DLP) tools enable the dynamic application of policy based on the content and context at the time of an operation. These tools are used to address the risk of inadvertent or accidental leaks, or exposure of sensitive enterprise information outside authorized channels, using monitoring, filtering, blocking and remediation features."

Several consultants have provided explanations of DLP. One helpful example is provided by Securosis at https://securosis.com/blog/new-paper-implementing-and-managing-a-dlp-solution. A useful independent overview of DLP vendors may be obtained from the DLP Experts: www.dlpexperts.com.

Identify Stakeholders + Priorities

2. A. Plan - Representation By All Stakeholders

Selected stakeholders within the organization need to be involved in order to provide sufficient knowledge of the organization's:

- Regulatory compliance requirements
- Current policies relating to handling sensitive information
- Present information storage and handling processes
- Information Technology assets

This knowledge will typically require input from:

- Physicians and staff
- Compliance and privacy personnel
- HR
- IT Security
- Administrative management
- Third party consultants specializing in DLP

While many individuals and groups may be involved, one person should be designated with coordinating authority and ownership of the project.

Gain the highest appropriate executive level commitment for this effort. This leadership will be needed as conflicts may arise during the final stages of decisions and as implementation will enforce changes in system user behavior. For example, often individuals are slow to accept changes that are of crucial importance to the organization.

2. B. Plan - Objectives and Priorities

Whether the organization is evaluating the implementation of DLP for the first time, or wants to evaluate or audit its already existing systems, developing an agreement on what the solution should accomplish is essential. DLP will meaningfully reduce the risk of loss of patient information across many potential channels of loss. However, it is critical to set a priority around network loss, endpoint loss, or loss, due to a file exposed on a file system.

In establishing these objectives it is important to keep in mind that DLP does not solve every security issue. But it should be a key component of managing the organization's overall security strategy and information governance. In other words, attempting to remove all risk is not a reasonable goal. A fair objective should be to reduce risk to a reasonable level based on the estimated costs and benefits.

Easy steps should be identified for implementation first. Very simple data loss prevention policies will yield very high returns very quickly. Some examples are discussed below.

2. C. Plan - Primary and Tangential Requirements

While protecting every patient's information is, of course, of paramount concern, there may be other related sensitive

data to be prioritized at the appropriate level for addressing with DLP. Examples of information that might or might not require particular management control could include:

- VIP patients such as politicians, well-known figures in the community, professional sports team members, Hollywood stars and children of the VIPs. Extremely sensitive patients may demand additional security measures be taken to ensure their personal information is protected.
- Large donors are required to provide their tax data to the institution. This information should not be improperly released without authorization.
- Employees may also be patients. In those cases it may be desired to not duplicate certain information.

2. D. Plan - Identify Unique Risks from Newer Technology

Gather and review policies and procedures concerning current or planned new technology areas of likely leakage concern. Establishing detailed plans in each of these areas should be developed carefully and with expert advice.

- **Mobile devices**
  Smart phones, tablets and various other communicating devices are convenient, growing in popularity and may at times be disconnected from the rest of the system. Moreover, bringing your own device (BYOD) for business purposes is a trend with momentum that will continue to grow. Being able to monitor and control the patient information being sent to and received by these devices is mandatory in today's environment.
- **Cloud storage**
  The cloud is increasingly under consideration for possible cost savings and expansion flexibility. With the different sort of risks it embodies this technology should be included in any discussions of plans for managing protected information. This should include the possibilities of both off and on-premise cloud use, as well as the possibility of an individual in the organization storing patient records on a personal cloud.

A recent study by the Poneman Institute (www. ponemon. org) a provider of statistical data on security breaches, revealed that' in the absence of strong policy, employees may consider using Classification Checklist potentially unsecured, free Web services to share patient data for access on their mobile devices". The convenience is understandable but the impact on HIPAA compliance makes this practice unacceptable.

Identify Stakeholders + Priorities

3. A. Select - Modular Solutions with Appropriate Costs

Ask questions. Avoid buying features you will never use. Seek a solution that is modular enough to provide what is needed and does not include unnecessary features (and costs) before they are useful. For example, look for an Enterprise DLP suite with multiple modules that can be purchased individually and yet allow consistent policies to be applied across the File Stores, Network or Endpoints. Avoid narrowly focused "solutions" that will address only a single channel, such as email, yet leave the organization exposed to leakage through other paths.

A 5 year Total Cost of Ownership (TCO) analysis should be developed at this point. This analysis should show the monthly, annual, and total costs for:

- Hardware
- Software
- Maintenance
- Training
- Professional services

Developing a TCO will require understanding the licensing policy of any vendor being considered. Determine if the software licenses will be purchased or must be paid for on an annual or monthly basis.

3. B. Select - Vendors and Consultants with Healthcare Expertise

Ask questions in order to understand any vendor's or a consultant's specific experience with healthcare information requirements and successful prior implementations. Some DLP solution providers use overly complicated polices. Others may rely on overly simple processes that must be tuned considerably for the Healthcare Environment.

Insist on a Proof of Concept (POC) demonstration done in your own environment with your own data. Evaluate potential solutions based around how easy the

demonstration is to set up and manage. Relying too heavily on "out of the box" solutions is likely to produce an unsatisfactory number of false alarms in practice.

Note that DLP serves a very different purpose than a firewall or mere encryption. DLP effectively combines business process, data, and security. A firewall has many standard polices that all organizations should simply enable without tailoring to a unique purpose.

Deploy - With An Iterative Methology

4. Deploy - With An Iterative Methology

DLP is a data management tool that will be most effective when applied in repeating stages. This means identifying easily won objectives and accomplishing those first, then assimilating what was learned and moving to the next goal.

Following such an outline will make the DLP implementation less disruptive to those affected and responsible for making it work. Progress will be easier to measure and the process easier to modify when needed.

Before initiating live controls, survey the overall situation:

1. **Identify Regulated Data to be controlled**
   For healthcare organizations, scanning for a simple combination of patient name and SSN or MRN is recommended as a starting data set to use. This set of data (though simple) will serve as a good marker for identifying PHI records in a scanned target. There are many methods to utilize DLP to discover where PHI is residing or being transmitted. For example, detecting HL7 or X12 protocols in outbound communications may be applicable in many cases.

2. **Identify potential places where this information might leak**
   For healthcare organizations it is recommended to inspect the following channels:

   - Email – Consider all outbound email traffic including attachments.
   - Web traffic – Gmail, and other web mail providers, Facebook and other social media sites should be monitored.
   - Other protocols – In particular unencrypted HL7 and X12 protocols should not be crossing the organization's firewall.
   - Data storage – Identify and categorize the information on all storage under control of the organization, including file servers, file shares, SAN, SharePoint servers, user home directories, workstations and laptops in order to determine the assets requiring review and inspection.
   - USB, DVD – Consider workstations that allow USB mass storage or DVD burning and any devices that can be physically disconnected and carried away.

3. **Scan data stores for regulated information**
   Once assets have been determined, identify any potential regulated or sensitive information on that asset. A DLP solution will assist in this step. For example, as a first step, identify all files containing a patient name plus medical record number. Or a list of all users sending emails containing patient name and MRN. Or a list of all files copied to USB devices that contain confidential information.

4. **Review any regulated data found**
   Review information uncovered in step 3. Is it permissible for PHI to be transmitted to the destinations it is going to? In particular in the case of large transfers, is this data being encrypted and sent to known partners? Is it acceptable for PHI to be on this network share? Is it allowed for this person to send this list of PHI to their email account?

5. **Apply controls**
   Once the data has been reviewed, controls can be instituted to reduce or prevent the potential loss of PHI. For example, notifying users via email every time they send an email containing PHI will reduce the amount of PHI sent simply because users now know that the transmission of PHI data is being monitored. PHI can be removed from network shares where controls are not adequate.

Repeat these steps until a satisfactory level of understanding is developed in the form of a map to the protected information and appropriate controls are in place and understood by the stakeholders and system users.

A major use of DLP is as the cornerstone of HIPAA Risk Analysis audits. At an early stage, conduct a mock HIPAA audit. Not only will you be ready if your organization is audited, but, it will force questions to be asked regarding where to focus on risk mitigation.

The Benefits

More than a security system, DLP is a valuable management tool once understood and properly deployed. Its benefits are centered on protecting against leaks of regulated information. However, an appropriate DLP solution may be applied to the broader context of security systems and overall policies for information governance.

This is particularly the case in health and financial information arenas. The suggestions made here, in particular, those suggesting a methodical and "easy steps at a time" approach are based on years of experience working with hospitals and other health organizations handling private medical information.

About Digital Guardian

Fortra™'s Digital Guardian® is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.