WHITE PAPER

DIGITAL GUARDIAN®

PROTECTING PATIENT DATA IN THE CLOUD

BEST PRACTICES FOR MIGRATING AND PROTECTING PATIENT DATA IN THE CLOUD

OVERVIEW

Healthcare and associated medical record handling organizations have been utilizing Data Loss Prevention (DLP) as a cornerstone in meeting legal requirements to protect regulated patient health information within their network. Now, as organizations have increasingly begun to utilize cloud computing to store and share patient information, questions have arisen as to how best to extend proven DLP solutions to include cloud storage as well. In this paper, best practices in applying DLP to the cloud are organized into the major stages in the process:

- Planning
- Migrating to Cloud Storage
- Ongoing Operation

The topics are directed toward organizations that may be considering DLP technology with cloud storage for the first time. However, any healthcare executive involved with regulated healthcare information compliance will find value here.

WHY IS THE CLOUD VALUABLE TO HEALTHCARE ORGANIZATIONS?

The cost and scalability benefits of the cloud are particularly substantial for many healthcare organizations which may have limited IT resource. With appropriate security the cloud may further enable more efficient and productive sharing of patient data between multiple care providers, their associates and the patients themselves. However, concerns over the loss of visibility of data in the cloud has prevented many organizations from seeking these benefits. Healthcare IT professionals may ask "how can we protect sensitive data if we lose visibility of where it is?"

WHAT ARE THE REQUIREMENTS TO PROTECT PATIENT INFORMATION?

The importance of managing patient medical information is dictated in the United States by Federal HIPAA/HITECH regulations familiar to all healthcare organizations. These regulations require, as just one example, that, whether data is encrypted or not, the organization must know where patient data is stored or sent. In other words, encryption, alone, is not enough to meet the necessary standards or to provide the visibility required to govern this type of sensitive data.

This paper outlines the selection and use of proper DLP to help address these requirements and significantly reduce the risks.

WHAT IS AT STAKE FOR HANDLERS OF PERSONAL HEALTH INFORMATION?

The improper release of regulated patient medical records can result in a drop in confidence by their patients and the general public as well as fines and penalties from the Health and Human Services regulatory agencies. Maintaining compliance with these regulatory acts is a vital concern for every organization handling electronic health records. In September of 2013 the HIPAA Omnibus ruling took effect, which, among other guidance, provided significant clarity in spelling out what is required of the Business Associates of a healthcare organization. In a nutshell, they are required to provide the same protection to personal health information as a covered entity.

7 STEPS FOR PLANNING TO MOVE PATIENT DATA TO THE CLOUD

The following steps will help any healthcare organization make appropriate decisions prior to deciding if they are ready to move regulated information to the Cloud.

1. Assess Current Information Policies - Insure that any existing information governance rules may be extended to cloud data. In some cases it may be desired to apply more stringent controls on data in or intended for cloud storage.

2. Assess Current Usage of Cloud Storage - Determine the protection requirements and status of any data already stored in the cloud. Investigate current personal cloud use by medical professionals or other employees. It may be found that some patient data is already being inappropriately stored in the cloud and creating data loss risks previously not known. An appropriate managed cloud capability will remove the perceived need for any such practices by individuals.

3. Establish Credible Expectations - Cloud storage changes the available means of data visibility and control. In the absence of a well communicated policy, medical professionals may use unsecured cloud services to store patient data in order to make it more easily accessible when traveling with their mobile devices. A DLP solution appropriate for cloud storage protection will facilitate the application of uniform policy across the enterprise, including the cloud. In particular, an appropriate DLP solution will provide means for educating every end user and preventing unauthorized actions when required by policy.

4. Set Objectives Appropriate for the Organization - After gathering and reviewing existing policies and procedures concerning the handling of sensitive information develop agreement on what information is to be placed in the cloud, what that placement should accomplish, and note any information requiring special protection and control. For example, a first step may be to identify and encrypt all records identifying patient names with their Social Security or hospital ID numbers.

5. Involve the Stakeholders - Ensure the participation of those responsible for entering or accessing patient information and those responsible for adhering to HIPAA compliance requirements. All parties should understand the benefits being sought from cloud storage and the requirements for protecting sensitive data expected to be placed there. Managers should understand the benefits and issues of the cloud storage as well as the policy enforcement capabilities provided by DLP. These persons could include:

   - Compliance and Privacy personnel
   - Professional medical staff
   - HR
   - IT Security
   - Executive management
   - Third party consultants specializing in Data Loss Prevention

6. Assess the Costs Involved - If DLP is being acquired for the first time, resist buying features you will never use. Do a 5 year Total Cost of Ownership (TCO) analysis to compare alternative possibilities, including the costs for: the hardware, the software, maintenance, training, and any professional services that will be required. Understand any software licensing payment terms.

7. Test Any Proposed Solution On-Site - Insist on a short demonstration or Proof of Concept to evaluate ease of installation and usage. This should be done in your environment with the organization's own data both inside and outside of cloud storage. A system that requires separate services only for cloud storage will be both inefficient and confusing

in operation. Seek a DLP solution capable of comprehensive and consistent compliance management across the enterprise including the cloud.

6 STEPS TO MOVING PATIENT DATA TO THE CLOUD

Once the decision is made to proceed with the cloud and DLP solution the following steps should be taken to prepare for and execute the migration of data to cloud storage. An appropriate DLP Discovery tool capable of performing these actions will ensure that regulated information will be properly identified, categorized and protected, or, removed before it may be uploaded and exposed to access in the cloud:

1. Scan Data Already in Cloud Storage - Use the DLP Discovery tool to inspect all previously stored information in the cloud to bring it under the same policy levels as will be applied to the newly migrating data. This will assure uniformity that newly adopted policy rules will be applied to any older data already placed in the cloud. Note that this important cloud Discovery capability is not a feature offered by every DLP provider.
2. Identify Assets for Migration to the Cloud - Identify information assets that are candidates to move the cloud. This will require identifying and categorizing the information on all storage under control of the organization, including file servers, file shares, SAN, SharePoint servers, user home directories, work-stations and laptops in order to determine the best candidates to move the cloud. For example it might be an easy decision to consider moving a marketing file to the cloud to facilitate sharing with an external design agency.

3. Scan the Identified Assets for Regulated Data - Once candidates have been selected for cloud migration the next step is to identify any potential regulated or other sensitive information on that information asset. An appropriate Data Loss Prevention (DLP) Discovery scan should be employed to carefully assess and, perhaps, remediate specific information assets prior to migrating them to cloud storage. An example might be to encrypt any files containing identifiable personal health information.

4. Review Any Regulated Data Found - The DLP Discovery scan will produce a list of potential regulated or sensitive information on each information asset. This output will help determine the actions required before moving the data on a particular information asset to the cloud.

5. Remediate Any Regulated Data as Appropriate - An appropriate DLP Discovery solution will include the ability to remediate potentially sensitive data both during and after the discovery scan. These include: moving files to secure vaults, deleting files, or applying rights management. If the objective is to move an information asset to a cloud storage provider then all regulated data should be moved to a secure area or simply removed altogether from that asset prior to moving the information.

6. Move the Information to the Cloud - Once the information asset has been sanitized it is ready for migration to a cloud storage provider. If the data has not already been sanitized then apply DLP to scan and block any regulated data found as it is in flight to the cloud.

4 STEPS TO KEEPING PATIENT DATA IN THE CLOUD PROTECTED

By selecting a DLP solution that provides coverage uniformly across the enterprise including cloud storage, the organization's ongoing management of regulated or other sensitive information is greatly simplified. Policies will be enforced with consistency and from single administrative control. Here are steps to help guide the ongoing processes:

1. **Audits -** At any time, conduct a mock HIPAA compliance audit involving the information in cloud storage. Not only will the organization be ready for any external audit demands, but this will force questions to be asked regarding where to focus next on risk mitigation strategies.

2. **Filter and Audit Information as it is Moved to the Cloud -** Apply Network DLP capabilities to inspect all data before it leaves the enterprise network and heads to the cloud. DLP tools will identify regulated information and allow it to be removed, encrypted on the fly, or stopped for remediation according to policy for the particular information. Note that this provides for information to be inspected at the final stage rather than some prior point where remedies could be undone at a later point. These automatic processes reduce opportunities for error and audit trails provide visibility into information being transmitted.

3. **Scan Files Systems Planned for Cloud Storage -** For efficiency it may sometimes be appropriate to scan entire file systems when there are uncertainties regarding content. Or, the file systems may be so large that it is desirable to scan them prior to the uploading transmissions, which will look at each record at a time. An appropriate DLP solution may be employed to inspect all data poised for sending to the cloud. Sensitive data discovered will be controlled according to policies established by the enterprise:

   - Before release to the cloud sensitive information may be denied passage or automatically encrypted
   - Or, other prescribed remediation may be applied

4. **Apply Remediation Selectively at Each Step -** It may or may not be most effective to encrypt-everything sent to the cloud. An appropriate DLP will allow, at every stage in the process, the appropriate remediation to be automatically applied according to the policies established by the enterprise for that particular information and where it is being stored or transmitted:

   - Policies dictate action for specific data elements
   - More efficient, speedier processing
   - Alternatives may add burden of needless repetitive encryption and decryption

IT'S ALL ABOUT THE DATA

Data Loss Prevention has proven to be an invaluable resource in protecting regulated personal health data as advances in technology has migrated information from secure data centers to distributed file servers to the desktop and to mobile computing devices. Now, with appropriate tools, this technology may be applied to data in the cloud as well.

There are many resources to assist organizations in sorting out the options available for data protection. But, the most important criteria for a healthcare organization is to evaluate solutions that will apply consistent and uniform policy enforcement to patient data across the entire enterprise, no matter where it is stored, including cloud storage. A good way to see this in action is to ask for proof of concept on site.

No single tool is capable of addressing every security issue; however, an appropriate DLP implementation will, by accurately identifying regulated data wherever it may be stored or sent, substantially reduce the risks to the healthcare organization as a key component of its overall data security strategy.

ABOUT DIGITAL GUARDIAN

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.

DIGITALGUARDIAN®

CORPORATE HEADQUARTERS
860 Winter Street, Suite 3
Waltham, MA 02451 USA
info@digitalguardian.com
781-788-8180
www.digitalguardian.com

SHARE