DATA PROTECTION

HIPAA

NETWORKS
CONSULTING RESOURCES

CONTENTS

INTRODUCTION

After reading this white paper, you will better understand the HIPAA data security standards so you can then compare your organization's security with the current requirements. You will also learn how our backup solution can help you become HIPAA compliant.

Patient privacy continues to be a chief topic of concern as technology continues to evolve. Now that the majority of patient information is transferred over to digital format, organizations realize that they are exposed to certain risks. These hazards include disaster that may cause physical damage to computers that store patient information, corruption by virus attacks, and even stolen data by unauthorized personnel.

Prior to the institution of the Health Insurance Portability and Accountability Act ("HIPAA") by Congress in 1996, there were no universal standards set in place to identify whether a healthcare provider was properly securing patient information. HIPAA was designed to promote the confidentiality and portability of patient records, as well as to develop standards for consistency in the health care industry. Under HIPAA, organizations adhere to standards related to protecting their systems, and patients can feel confident that their personal medical information will remain private.

This act applies to any health care provider, health plan or clearinghouse (collectively "Covered Entities") that electronically maintains or transmits health information pertaining to patients. If you are a Covered Entity, you must establish appropriate measures that address the physical, technical and administrative components of patient data privacy. The Security Rule requires health care providers to put in place certain administrative, physical and technical safeguards for electronic patient data. Among other things, Covered Entities are required to have a Data Backup Plan, a Disaster Recovery Plan, and an Emergency Mode Operation Plan.

Why should your organization be concerned with this compliance? In 2009, Congress passed the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which implemented stricter penalties for HIPAA violations and expands the organizations bound by HIPAA regulations to include business associates of medical offices.

Business associates include software vendors providing EHR (Electronic Health Records), though there is room within the law to interpret other potential parties responsible for upholding HIPAA standards.1 If you are a health care provider or handle health information pertaining to patients, ensuring that you observe HIPAA rules is necessary for your business. By complying with HIPAA standards, you can maintain trust with your customers and prevent security breaches as well as financial loss.

What happens to organizations that do not secure their electronic protected health information? HIPAA carries serious penalties for non-compliance. Civil penalties for willful neglect under the HITECH act can extend up to $250,000 with repeat/uncorrected violations up to $1.5 million.2 Criminal penalties range from $50,000 in fines and one year in prison up to $250,000 in fines and 10 years in jail. Non-compliant organizations also face losing customers and business partners who refrain from working with companies who do not sufficiently safeguard their electronic protected health information. Additionally, these organizations can suffer from negative publicity and legal liabilities.

HIPAA SECURITY RULE

The Security Rule applies to protected patient health information in electronic formats. This is protected patient information either transmitted by electronic media or maintained on electronic media. Covered entities that maintain or transmit protected health information are required by the Security Rule (see 45 C.F.R. §164.306) to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the Covered Entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- Ensure compliance with this subpart by its workforce.

According to the HIPAA regulations, Covered Entities are allowed to use a flexible approach when implementing the above requirements. Specifically, Covered Entities may use any security measures that allow the Covered Entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

In deciding which security measures to use, a Covered Entity must take into account the following factors:

- The size, complexity, and capabilities of the Covered Entity.
- The Covered Entity's technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to electronic protected health information.

With this information in mind, organizations must adhere to the Security Rule's standards and specifications for backing up and safekeeping electronic data. Covered Entities also need to institute a contingency plan to be prepared for an emergency, such as a natural disaster or computer virus attack that results in a major data loss. The contingency plan must:

- 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 (Administrative Safeguards - §164.308(a)(7)(i)).

This contingency plan must be implemented as follows:

- Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
- Disaster recovery plan (Required). Establish and implement procedures to restore any loss of data.
- Emergency mode operation plan (Required). Establish and implement procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

HIPAA SECURITY RULE

Covered Entities must also have certain physical safeguards, such as facility access controls. They must:

- Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed (Physical Safeguards - §164.310(a)(1)).
- The contingency operations should establish and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency (§164.310(a)(2)(i)).
- In addition, Covered Entities must implement specific technical safeguards (§164.312) to, among other things:
- Limit access to and electronic protected health information.
- Encrypt and decrypt electronic protected health information.
- Put into place audit controls that record and examine activity in information systems that contain or use electronic protected health information.
- Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

These regulations are in place to ensure that healthcare organizations properly secure their electronic protected health information. Based on these directives, an organization should evaluate their system and then implement a secure backup, archiving and recovery solution to comply with HIPAA standards.

THE HIPAA OMNIBUS RULE

Announced January 17, 2013, the HIPAA final omnibus rule implemented a number of new privacy protections, expanding some of the obligations of Covered Entities to “Business Associates”, the definition for which was also expanded under the omnibus rule.

As defined by the Department of Health and Human Services (HHS), “Business Associates” are defined as “a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.” HHS provides the following examples of Business Associates:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.

HIPAA includes a “conduit exception” for business associates, exempting businesses that “only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law.”

As part of the omnibus rule, the conduit exception was further restricted to eliminate the exception for organizations that maintain EPHI, such as cloud backup or data storage providers.
As a result, cloud backup and online data storage providers are liable for HIPAA as business associates, and must enter into a “Business Associate Agreement” with the covered entities they serve. According to HHS, this contract must:

- Describe the permitted and required uses of protected health information by the business associate
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law

Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract3.

HIPAA COMPLIANCE AND INTRONIS BACKUP

Intronis Backup can help organizations meet HIPAA compliance requirements, specifically those of the Security Rule. It is a cloud backup, archiving and recovery solution that automates the process of securely backing up electronic data and file recovery. It was created, with healthcare providers in mind, to satisfy the broad need for a safe, reliable, and cost-effective method of backing up data offsite and allowing full file restoration at any time from any authorized location.

The Intronis Backup solution ensures that all electronic protected health information is fully protected when it is backed up and stored. It encrypts all data and stores the information in military-grade facilities. The HIPAA security standards require your practice to appoint someone as the security manager, thus only this designated individual in charge of the security management process will have access to this data, hence preventing unauthorized access or corruption. Furthermore, in the event of a natural disaster or system failure, the data will be recoverable, thus, assuring that patient medical records will not be lost.

SECURITY AND ENCRYPTION

Why is it important to secure and encrypt your data?

Businesses need to protect electronic protected health information from unauthorized access and corruption. David Kibbe of the American Academy of Family Physicians explains, "The basic idea behind cryptography, of which electronic data encryption is a branch, is that a group needs to keep a message secret from everyone else and therefore encrypts it. Encryption is the transformation of a message from plain text into nonsensical cipher text before the message is sent. Anyone who steals the cipher text message will not be able to understand it.

Only those who have the code used to encrypt the message can convert it back from cipher to plain text and reveal its meaning."[4]

The following types of electronic data contain information that should be encrypted when backed up:

- Patient billing and administrative information exchanged with payers and health plans;
- Utilization and case management data, including authorizations and referrals that are exchanged with payers, hospitals and utilization management organizations;
- Patient health information gathered from or displayed on a Web site or portal;
- Lab and other clinical data electronically sent to and received from outside labs;
- Word-processing files used in transcription and other kinds of patient reports that are transferred electronically;
- E-mails between physicians and patients, and between attending and referring physicians and their offices.

The Intronis Backup solution is a secure and trusted method to protect this private data. During a backup, all data – including patient and billing records – will be encrypted before leaving the user's computer(s) and is never accessible without the user's encryption key. This encryption key is stored only on the user's system and never transmitted over the Internet. Furthermore, it is not stored on the Intronis Backup servers, thus no one but the user in possession of the key can access files or even read the file names. Only the encryption key holder maintains control of their data, eliminating the threat of unauthorized access.

Data is encrypted using a 256-bit Advanced Encryption Standard (AES) encryption technology. AES encryption was developed by the U.S. National Institute of Standards and Technology (NIST) and is now the state-of-the-art standard encryption technique for both commercial and government applications. Moreover, in June 2003, 256-AES was approved by the United States National Security Agency (NSA) for use encrypting the U.S. government's documents classified "TOP SECRET." Using this secure technology, data is initially encrypted during the initial backup and then encrypted once again during the Internet transfer, to and from the Intronis Backup servers.

For added security, and to meet the Security Rule's transmission requirements, each encrypted file is sent over the Internet via a secure channel using Secure Sockets Layer (SSL) technology. The same Internet transmission technology is used for online banking and credit card applications. As a result, Intronis Backup is able to provide double the data encryption of typical cloud backup products.

Additionally, all user data is transferred and stored in two redundant, Level 4 SSAE 16 compliant secure data centers, located thousands of miles apart from each other. Each data center has 24/7 onsite monitoring, advanced security technology such as biometric access controls, backup generators and redundant connections to the Internet.

LOGGING AND ARCHIVING

Intronis Backup records each file that is backed up or restored as well as additional information and statistics regarding the backups. This audit log, which can easily be searched, allows the user to verify that files were successfully backed up and help troubleshoot any issues. The service provider also has the option to receive an automated email notification at the conclusion of each successful backup. Information about recent backups and total storage usage can also be viewed via the Internet, by logging on to the user's account at manage.intronis.com. For further HIPAA compliance, hard drives of the encrypted data are available for additional archiving.

BACKUP AND RESTORING

The backup process and file recovery process are completely automated, eliminating the need for manual data handling. Backups will automatically occur according to the specific schedule that the user sets in place as long as the computer is on and functioning (not in sleep or hibernate). Backups can also be initiated by the user at any time.

Restoring files can be accomplished with just a few clicks of the mouse by the individual who is designated as having overall responsibility for the security of a CE's electronic protected health information. Using Intronis Backup, the user simply chooses the files, folders or revisions to be retrieved by clicking on the file name. The data will then be downloaded to the user's computer, decrypted, and then restored to their original location or another specified location on the user's system. A password is required to restore any files, thus, preventing unauthorized restores, as per the HIPAA Security Rule.

In the event of a complete system failure, a full recovery of the user's backed up data can be initiated in just minutes. The recovery procedure can be performed on any Windows based computer - not just the computer where the data was originally backed up. The encryption key holder can simply download and reinstall the software, enter a username and password, and then enter the encryption key. Once the software installation is complete, the file catalog – the list of all of the files backed up – which will allow the user full control to restore their data.

HIPAA AND YOUR ORGANIZATION

“The biggest challenge presented by HIPAA is to accurately and consistently protect individuals’ privacy without crippling your business,” said Christopher Fuller of TechRepublic.5 To adhere to the standards stated in the HIPAA act while also streamlining the implementation process, consider Intronis Backup. It is the ideal solution for fully automated backups and optimum data security.

Get on the path toward HIPAA compliance by visiting yourwebsite.com or arrange for a personal consultation by emailing sales@yourmspcompany.com.

Please note that nothing in this white paper is intended to constitute legal advice. For more information about HIPAA and compliance with HIPAA requirements please consult your legal counsel.