Ensuring HIPAA Compliance with DISTINCTION

Online Backup and Archiving Services

from

Mahaska Data Technologies, L.L.C.

Introduction

Patient privacy has become a major topic of concern over the past several years. With the majority of patient information being transferred over to digital format to improve the convenience, efficiency and cost of storing the data, organizations expose themselves to certain risks. These risks include the possibility of damage to the computers storing the information by natural disaster or human mishandling, 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 or not a healthcare provider was properly securing patient information. HIPAA was designed to reduce the administrative costs of healthcare, to promote the confidentiality and portability of patient records, to develop standards for consistency in the health care industry, and to provide an incentive for electronic communications. With these standards in place, organizations better protect their systems, and patients can feel confident that their personal medical information will remain private.

Virtually all healthcare organizations are affected by the HIPAA standards. 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. With the exception of small health plans, all Covered Entities must have had data security standards in place and operational by April 21, 2005, when the Standards for the Security of Electronic Protected Health Information (the "Security Rule") of HIPAA went into effect for health care providers. Small health plans were exempted until April 21, 2006. 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 will be 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? Simply put, every patient cares about the privacy and integrity of their health information. More and more people are becoming aware of their rights to keep that data private and are taking action when that data is compromised. With today's dilemma of identity theft, protecting personal information

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

stored in digital format is critical. Baseline magazine reports that more than 90 percent of data breaches in 2006 were in digital form and some 40 percent of publicly disclosed security breaches were caused by hackers or insider access, specifically targeting sensitive personal information [1]. The FBI reported in 2006 that the average cost per data breach has reached $4.8 billion and since February 2005, 93.8 million personal records have been reported lost or stolen. With these statistics in mind, you see that not only is data protection vital in protecting individual patients, it is also cost-effective for organizations. By complying with HIPAA standards, you can prevent security breaches to maintain trust in your customers as well as avoid financial loss.

What happens to organizations that do not secure their electronic protected health information (EPHI)? HIPAA is now the law and carries serious penalties for non-compliance. Civil penalties are $100 per violation, up to $25,000 per year for each requirement violated. 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 other serious consequences such as losing customers and business partners who refrain from working with companies who do not sufficiently safeguard their EPHI. Additionally, these organizations can suffer from negative publicity and legal liabilities.

After reading this white paper, you will better understand the HIPAA data security standards and can then compare your organization's security with the current requirements. You will also learn how Distinction online data backup, archiving and recovery service complies with HIPAA and can help you take a proactive approach to securing your organization's private data.

The 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:

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

• 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)).

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

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.

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 any 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.

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

These regulations are in place to ensure that healthcare organizations properly secure their Electronic Protected Health Information (EPHI). 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.

HIPAA Compliance and DISTINCTION Software

Distinction online backup from Mahaska Data Technologies, L.L.C. (MDT) can help organizations meet HIPAA compliance requirements, specifically those of the Security Rule.

Distinction, from MDT, is an online backup, archiving and recovery solution that automates the process of securely backing up electronic data and file recovery. **Distinction** 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 solution was designed to encompass the advanced functionality and features of backup systems used by Fortune 500 companies, yet be effortless for anyone to use regardless of their computer expertise.

The solution ensures that all electronic protected health information (EPHI) is fully protected when it is backed up and stored. The software encrypts all data and stores the information in military-grade secure facilities. The HIPAA security standards require your practice to appoint someone as the security manager[3], 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.

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

DISTINCTION
Security and Encryption

Why is it important to secure and encrypt my organization's data?

Your organization needs to protect EPHI 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." 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 [3].

The solution offers 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

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

encryption key is stored only on the user's system and never transmitted over the Internet. The backup is not stored on MDT servers, thus MDT cannot access files or even read the file names. Only the user maintains control of their data, eliminating the threat of unauthorized access.

The solution encrypts data 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 State's 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.

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, **Distinction** is able to provide double the data encryption of typical online backup products.

Additionally, all user data is transferred and stored in two redundant Level 4 secure data centers, located hundreds 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.

DISTINCTION

Logging and Archiving

The software 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 user also has the option to receive an automated email notification at the conclusion of

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

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. For further HIPAA compliance, CDs and DVDs of data are available for additional archiving.

Backing Up, Restoring with DISTINCTION Managed Backup Services

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 the user sets in place as long as the computer is on and functioning (and not in sleep or powersave mode). Backups can also be initiated by the user at any time. Because backups run in the background of the system, they have little or no impact on the computer's performance or Internet connectivity, and are non-disruptive.

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 EPHI. Using the solution, the user simply chooses the files, folders or revisions that he or she wants to retrieve 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 user can simply download and reinstall the software, enter his /her username and password, and then enter the encryption key. Once the software installation is complete, the file catalog can be

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

accessed (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," exclaims Christopher Fuller of TechRepublic. To adhere to the standards stated in the HIPAA act while also streamlining the implementation process, consider the **Distinction** online backup, archiving and recovery service. **Distinction** is the ultimate solution for fully automated backups and optimum data security. Get on the path toward HIPAA compliance and contact us to arrange for a personal demonstration.

Mahaska Data Technologies, L.L.C. • 114 A Avenue East, Oskaloosa, Iowa 52577
Phone: (641) 673-5959 Toll-free: (855) 673-5959
On The Web: www.mahaskadatatech.com

About
Mahaska Data Technologies, L.L.C.

Our mission is to provide *great* software and software services to clients in Oskaloosa and southeast Iowa. We have been doing that almost eight years.

Our office is located near the heart of Oskaloosa, at 114 A Avenue East. Our contact information is:

Phone: (641) 673-5959

Toll-Free: (855) 673-5959

eMail: info@mahaskadatatech.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.

[1] Deborah Gage and Kim S. Nash, "Case Dissection: Serious Pain," Baseline, December 2006

[2] Ponemon Institute, PGP, and Vontu, op. cit., p. 3

[3] David C. Kibbe, "10 Steps to HIPAA Security Compliance," American Academy of Family Physicians, April 2005