HIPAA Information You Can Use

The word “HIPAA”, otherwise known as Health Information Portability and Accountability Act, has caused many a headache in the health care community for the past few years. Now that some of the standards are in effect, and others will be soon, there is a lot of necessary information to learn and understand. We trust this information will be helpful to you and aid you in figuring out the mazes of HIPAA. Enjoy reading!

Your Document Management Solution Providers,

Triangle Solutions Technology, LLC

Safeguard and Security

There are many concerns about what must be done to meet compliance for both the Privacy and Security Standards. This article sheds some light on what may be acceptable safeguards for the Privacy Standard and provides some clarification on the Security Standard.

Privacy Standard

Under the HIPAA Privacy Standard, covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information (PHI). PHI is individually identifiable health information transmitted or maintained in any form or medium, which is held by a covered entity or its business associate.

The HIPAA Privacy Rule does not prohibit covered entities from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual’s privacy while engaging in these practices. Covered entities must review their own practices and determine what steps are reasonable to safeguard their PHI. In addition, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to PHI. The Privacy Rule does not require that all risk of PHI disclosure be eliminated. In determining what is reasonable, covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguards to their particular circumstances.

For example, the Privacy Standard does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual’s privacy:

- Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., “high fall risk” or “diabetic diet”) at patient bedside or at the doors of hospital rooms.

  Possible safeguards may include: reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.

Inside You’ll Find…

Triangle Solutions Technology, LLC
3594 Old Fairground Road, Angier, NC 27501
Phone: 919-873-9996 ▲ Email: tst@trianglesolutions.com ▲ URL: www.trianglesolutions.com

Safeguards and Security

Who is in charge of enforcing the HIPAA standards?

The Department of Health and Human Services (HHS) has determined that the **Centers for Medicare & Medicaid Services** (CMS) will be responsible for developing and enforcing the Administrative Simplification requirements of HIPAA. A new office within CMS, the Office of HIPAA Standards, was created to proactively support and oversee the following requirements:

- **Transaction and Code Set**
- **Security**
- **National Identifier**

The HHS' **Office for Civil Rights** (OCR) will continue to oversee and enforce the **Privacy requirements**.

How will CMS enforce the Transaction and code sets standard?

The enforcement of the transaction and code sets is primarily complaint-driven. When CMS receives a complaint about a covered entity, they will notify the entity in writing that a complaint has been filed. The entity will have the opportunity to demonstrate compliance or to submit a corrective action plant. Organizations that exercise "reasonable diligence" and make efforts to correct problems and implement the changes required to comply with HIPAA are unlikely to be subject to civil or criminal penalties. However, if the covered entity does not respond to CMS, fines could be imposed as a last resort.

- Announcing patient names and other information over a facility's public announcement system.

  Possible safeguards may include: limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.

The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.

Security Standard

As the health care industry evolves and continuously relies upon the use of technology, the Security Standards will play an important role in protecting electronic data at rest and in transit. The standards were developed to promote the protection of electronic protected health information by:

- providing for electronic data integrity and confidentiality,
- allowing only authorized individuals access, and
- ensuring its availability.

The Security Standards are scalable and technology neutral. This means that covered entities should take into account their size, complexity, capabilities and potential risks to their electronic Protected Health Information when complying with the standards. The standards do not specify any particular technology. In other words, they outline what **must be done – not how to do it**. The Security Standard requires covered entities to implement safeguards within three categories:

- Administrative safeguards – management of the selection and execution of security measures.
- Physical safeguards – protections for electronic systems and related buildings and equipment from environmental hazards and unauthorized intrusion
- Technical safeguards – automated processes to protect data and control access to it.

In the Security Standards rule, both "required" and "addressable" implementation specifications were adopted. The concept of "addressable implementation specifications" was introduced to provide covered entities additional flexibility with respect to compliance with the security standards.

A covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. **The decisions that a covered entity makes regarding addressable specifications must be documented.**

Summary

With both the Privacy and Security Standards, safeguards and security work together. Covered entities put safeguards in place to provide security of PHI that fit the particular needs of their facility while meeting the requirements of both standards. As you continue dealing with HIPAA, document everything you do dealing with meeting HIPAA standards.

Triangle Solutions Technology, LLC
3594 Old Fairground Road, Angier, NC 27501
Phone: 919-873-9996 ▲ Fax: 919-873-9998 ▲ Email: tst@trianglesolutions.com ▲ URL: www.trianglesolutions.com

Document Management's Role In HIPAA

Westbrook Technologies' document management products, such as Fortis, streamline processing, allow for collaboration and provide security for documents throughout healthcare entities such as doctor's offices, clinics, HMOs, hospitals and pharmacies.

There are aspects of HIPAA that have no connection whatsoever to a document management initiative. However, those aspects that do deal with document management, Fortis can help. Read on to see how.

Security of Patient Documents and Information

Fortis' security model is of the highest integrity.

- Users must be authenticated before access is permitted.
- Access can be restricted at different levels, giving only authorized people access to confidential documents within a patient's folder.

This adheres to HIPAA rules that require information be protected from improper access or alteration.

Track Records with Audit Trail

Fortis users have the ability to track every aspect of the patient record. They can:

- Track who viewed a document and when they viewed it.
- Determine who e-mailed, who printed, and who faxed a patient record.
- See when patient information was scanned into the system, who scanned it, who viewed it after it was scanned, etc.

Audit Trail helps enforce rules that state users must account for each disclosure of a patient record.

Fortis Office Option

This option allows correspondence and forms created in Microsoft Word, Excel, and Outlook to be forwarded into patient records stored in Fortis. Data that is not paper based can be effortlessly included inside the same protected repository as all other documents; helping to ensure that patient information remains in a secure location.

What Does This Mean for Healthcare Organizations?

Regardless of where patient information originates: scanned from hard copy, faxed, emailed, PC-based or mainframe-based, Triangle Solutions and Westbrook Technologies provide a secure repository that can track all aspects of patient information.

To learn more information about Fortis and managing your paper and electronic records, contact a Triangle Solutions Technology representative at 919-873-9996 or via email at: tst@trianglesolutions.com.

Also visit our web site at: www.trianglesolutions.com

Document Management Return On Investment

Using a document management system can help:

- Reduce costs associated with copying and retrieving health information.
- Ensure aspects of your system are compliant.
- Tightly control health information while still providing more accessibility to those who need it.
- Protect data.

TRIANGLE SOLUTIONS TECHNOLOGY

www.trianglesolutions.com

Triangle Solutions Technology, LLC
3594 Old Fairground Road, Angier, NC 27501
Phone: 919-873-9996 ▲ Fax: 919-873-9998 ▲ Email: tst@trianglesolutions.com ▲ URL: www.trianglesolutions.com

HIPAA Deadlines and Helpful Links

HIPAA Deadlines: Some Have Passed and More are Coming

Post this table somewhere to keep yourself posted on the upcoming deadlines so you can stay ahead and be compliant. If your healthcare facility is not yet compliant with the HIPAA Privacy or Transaction and Code Set Standards, START NOW!

CMS is the acronym for Center for Medicare & Medicaid Services (CMS) and OCR is the acronym for the Office of Civil Rights.

HIPAA Deadlines	Description of Deadlines for HIPAA Requirements	Enforced By
October 15, 2002	*Transaction and Code Set Standards* deadline to submit a compliance extension form	CMS
October 16, 2002	*Transaction and Code Set Standards* - All covered entities except those who filed for an extension and are not small health plans	CMS
April 14, 2003	*Privacy Standard* - All covered entities except small health plans	OCR
April 16, 2003	*Transaction and Code Set Standards* - All covered entities must have started software and systems testing	CMS
October 16, 2003	*Transaction and Code Set Standards* - All covered entities who filed for an extension and small health plans must now comply to these standards Medicare will only accept approved electronic claims; paper claims accepted under limited circumstances.	CMS
April 14, 2004	*Privacy Standard* - Small health plans must be compliant	OCR
July 30, 2004	*Employer Identifier Standard* - All covered entities must be compliant except small health plans	CMS
April 21, 2005	*Security Standard* - All covered entities must be compliant except small health plans	CMS
August 1, 2005	*Employer Identifier Standard* - Small health plans must be compliant	CMS
April 21, 2006	*Security Standard* - Small health plans must be compliant	CMS

Check It Out!

HIPAA Information Series for Providers is a series of 10 newsletters that give very helpful information for HIPAA compliance. Download and read this valuable information:
http://www.cms.hhs.gov/hipaa/hipaa2/education/infoserie/

The Office of Civil Rights (OCR) has a great deal of information on the **Privacy Standard** at their web site: http://www.hhs.gov/ocr/hipaa/

The Center for Medicare and Medicaid (CMS) has important information on the **HIPAA Administration Simplification** for the Transaction and Security Standards. Go to their web site:
http://www.cms.hhs.gov/hipaa/hipaa2/default.asp

Only transactions in HIPAA Standard formats will be accepted after October 16, 2003. It will be required by most health care providers to submit Medicare forms electronically to CMS. Learn more about it at this web site:
http://www.cms.hhs.gov/providers/edi/

TRIANGLE SOLUTIONS TECHNOLOGY

www.trianglesolutions.com

Triangle Solutions Technology, LLC
3594 Old Fairground Road, Angier, NC 27501
Phone: 919-873-9996 ▲ Fax: 919-873-9998 ▲ Email: tst@trianglesolutions.com ▲ URL: www.trianglesolutions.com