Advisory

http://www.purdue.edu/hipaa

Included in this newsletter is guidance on various HIPAA-related topics that impact your everyday work life. Hopefully, it will help answer some of your questions about how HIPAA relates to your work processes.

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: http://www.purdue.edu/hipaa or contact: Joan Vaughan, HIPAA Privacy Officer telephone: (765) 496-1927 e-mail: hipaa-privacy@purdue.edu

HIPAA Uses and Disclosures of Protected Health Information

Derived from guidance provided by the Office for Civil Rights

The HIPAA Privacy Rule establishes a foundation of Federal protection for personal health information, carefully balanced to avoid creating unnecessary barriers to the delivery of quality health care. To avoid interfering with an individual’s access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

A covered entity may, without the individual’s authorization, use or disclose protected health information for its own treatment, payment, and health care operations activities.

For example:

- A clinic may use protected health information about an individual to provide health care to the individual and the primary care provider may send a copy of an individual’s medical record to a specialist who needs the information to treat the individual.
- A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.
- A health plan may use protected health information to provide customer service to its enrollees, however, Human Resource employees who make employment decisions are not allowed access to employee health information.
- A covered entity may disclose protected health information to another covered entity or a health care provider (including providers not covered by the Privacy Rule) for the payment activities of the entity that receives the information.

For example:

- A physician may send an individual’s health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.
- A clinic may give a patient’s payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment services.

A covered entity may disclose protected health information to another covered entity for certain health care operation activities of the entity that receives the information if:

Each entity either has or had a relationship with the individual who is the subject of the information, and the protected health information pertains to the relationship; and the disclosure is for a quality-related health care operations activity or for the purpose of health care fraud and abuse detection or compliance.

For example:

A health care provider may disclose protected health information to a health plan for the plan’s Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.
Cloud Computing in a Nutshell

What is it?
Cloud computing is the use of computing resources that reside on a remote server and are delivered to the end user as a service over a network or the internet by a third party service provider.

Why am I writing about it?
As we choose to move more services to cloud providers, we need to conduct due diligence on that choice and understand the impact it may have on our organization and our data.

Pros:
Cost savings: Storing data or running applications in a cloud environment can reduce costs enormously. Not only is money saved on the server infrastructure, software purchasing and licensing, backup hardware and software, but also in requiring personnel with expertise to manage servers, backups, etc. (This point can be debatable. The company will continue to pay fees monthly or yearly and never own anything)

Disaster recovery: Cloud storage is remote to your physical location, so places the data outside of your local disaster zone. Cloud providers also generally backup the data to another server for their own backup and recovery.

Robust: As cloud services are usually their only business, these companies are able to invest in much more robust architecture than an individual business would be able to afford.

Scalability and Performance: Cloud providers are able to scale quickly as your needs grow.

Quick Deployment: Without the need to design, build, and configure your own systems, deployment to a cloud system is very quick.

No more worrying about storage capacity. A cloud service is very elastic and able to accommodate growth quickly.

Location Independence: It doesn’t matter where you are located; you’ll be able to access your data and applications in the cloud service as long as you have an internet connection.

Cons:
Privacy and Security: A cloud provider’s reliability is critical. You are giving away private data and information, some of which is sensitive, restricted, and protected. It is up to the cloud service provider to manage, protect, and retain this data.

Vendor lock-in: Because you may be using a vendor’s app and storing data there, it can be difficult and painful to transfer data sets to another provider and migrate to a new application.

Downtime: There can still be a downtime instance of a server, or internet access may be interrupted due to a denial of service attack or other issue. Business continuation plans are still needed.

Increased Vulnerability: Cloud based solutions are exposed to the public internet and are therefore a more attractive target for hackers. Even the best have suffered security breaches.

Questions to ask a Cloud Provider before signing on the dotted line:
• Can you demonstrate similar implementations to our requirements?
• Will our data only be stored in the USA? Many cloud providers are overseas where Privacy laws are different.

HIPAA Disclosures...continued

Minimum Necessary. A covered entity must develop policies and procedures that reasonably limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. However, covered entities are not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes. A covered entity also is required to develop role-based access policies and procedures that limit which members of its workforce may have access to protected health information for treatment, payment, and health care operations, based on those who need access to the information to do their jobs.

Purdue is designated as a hybrid entity. This means that disclosures of or access to an individual’s PHI must only occur between providers with a treatment relationship with the individual or to Purdue staff who are providing payment (e.g. business offices paying for employee travel immunizations), payment services (e.g. accounts receivable) or healthcare operations services to one of Purdue’s covered clinics or Purdue’s health plans. HIPAA-covered providers and others with the legitimate need to use PHI, have an obligation to only disclose this information for purposes allowable under the HIPAA Privacy Rule, even if the information is available publicly by other means. If you are workforce of a covered entity an learn about information through the work that you do, you are obligated to protect it.

Covered areas at Purdue can be found at: http://www.purdue.edu/hipaa/primary_menu/guidelines/components/index.shtml

The definition of healthcare operations can be found at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html

If you have questions about allowable disclosures, please talk to your area HIPAA liaison (http://www.purdue.edu/hipaa/secondary_menu/administration/lienios/hipaaliaisonroster.pdf) or contact Purdue’s HIPAA Privacy Officer at: hipaa-privacy@purdue.edu or x61927.

• Do you have flexible contract agreements? Is there a yearly exit option in our contract?
• Do you have a Service Level Agreement?
• Are there multiple companies residing on the same server? How are we protected from one another?
• Please tell me about your disaster recovery plan and testing.
• How are you addressing HIPAA compliance? Have you had an external audit completed? (such as an SSAE 16) If not, can we review your most recent risk assessment?
• What type of connection will be used during our data entry into the cloud service? (What type of encryption?)
• What happens to our data at end of contract?

For more information about cloud computing:

Cloud Security Alliance Guidance
Cloud Security Readiness Tool

Purdue University is an equal access/equal opportunity university