COST EFFECTIVE TECHNIQUES FOR PRIVACY RULE COMPLIANCE

Jaspinder Grewal,
University of Chicago, Booth school of Business
grewal@chicagobooth.edu
Phone: (312)388-0770

What does it mean for organizations

- The philosophy “ Patient information is patient’s right and our duty as caregivers”
- Make sure that confidential and protected health information, doesn’t get exposed others who don’t need it or can misuse it.

Consequences of PHI misuse

- Stolen PHI negatively affects the social lives of patients
- Loss of customer and potential future customers
- Bad word of mouth among people
- Bad press, affecting the company's market competitiveness

Conducting a Security risk assessment

- It is different from IT security audit or general risk assessment
- It involves the survey of the whole organization
- Start small and gather data through surveys and interviews (take the evidence based management approach)
- Talk to the users of patient data

What to ask

- Do you encounter patient data at work?
- How regularly you deal with patient data?
- Do you send/ exchange patient data with others?
- How frequently and what kind (paper or soft copy)?
- Do you send data outside the organization?

Where to look

- Some areas where non compliance may occur :
  - Physicians using insecure email
  - Researchers dealing with patient data
  - IT exchange with vendors
  - Business associates and insurance providers
  - Stolen laptops and storage drives
- **New threats** :Smart phones and hand held devices that have ability to download email, can be stolen and data can be exposed

What to determine

- Number of users that need to be compliant, then we can determine feasibility of various available systems
- Do the users understand the risk and liabilities of non compliance
- Educating the users to be fully compliant in the future

"We have this great tool, but nobody uses it" - IT Department

Situational vs. Dispositional factors

"We have this great tool, but nobody uses it"

Where is the compliance philosophy?

- We need to understand that **provisioning** the **right tools/ technology** (creating a situation) for the employees to be compliant is a big part in high compliance rates.
- **Improving the situation:**

- The customer service philosophy: "What if it was me?"
- Tools: Easy to use and proper usage training.
- Training: Reasons for compliance and consequences of non compliance

Tools for organizations

Zipping tools with data encryption ability

- Low cost solution, Good for small organizations with limited number of users
- Encrypts data (128/256 bit)before being transferred
- Has a plug-in for Outlook, usually referred to as “Email companion”
- Best practice: Send two emails

Tools for organizations

Enterprise Email encryption solutions

- Installed at enterprise level, no user upgrades needed
- Encrypts email on the fly, no software needed for sender or receiver
- Easy to set central policies for all users (encrypt only attachment messages or all messages etc.)
- More expensive, large user base verifies cost

Tools for organizations

Secure FTP site

- Another low cost solution
- Upload files to a secure location and send download info to the user
- Again, send two emails, one for download link and another for password

Tools for organizations

Storage Media encryption

- Encrypts all or specific content on your machines hard drive
- Covers laptops, hard drives and USB drives
- Very useful for consultants and road warriors

Ending notes

- Talk to the people accessing PHI and make sure they understand need of compliance
- Audit for potential non compliance and use the tool best suited to the needs of your organization
- Watch out for device theft (laptops, smart phones, USB Drives)
- In the end, lets talk about Health Information exchanges setups