HIPAA Training

- PRIVACY
- CONFIDENTIALITY
- SECURITY
- AUTHORIZATION/CONSENT
- CONSENT: IMPLIED/EXPRESSED
- "MINIMUM NECESSARY RULE" AND "NEED TO KNOW BASIS"
- NOTICE OF PRIVACY PRACTICES

HIPAA Privacy Rule

- Effective Date: April 14, 2003
- OCR: oversees HIPAA privacy compliance
- CMS oversees HIPAA security compliance
- **PHI: Protected Health Information**
- Covered Entity (CE)
- Business Associate (BA)
- **Relationship with Health Information**
- Applicability
- **De-identification**

HIPAA Security Rule

- Applicability

- **Safeguards**:

-Administrative

-Physical

-Technical

- **Contracts** must be in place

The Omnibus Final Rule

- 563 pages long
- Effective Date: March 26, 2013
- Compliance Date for HIPAA CEs and BAs: September 23, 2013
- Enhancements: consumers privacy protections,

Understanding Breaches

- Chatting about consumers in **public places** (Cafeteria, elevators, lobby, waiting area)
- Social networks: Facebook, MySpace, Twitter, etc..
- Portable devices: Cell phones, laptop, flash drive,…
- Emails: **Encryption**/Decryption(Phishing)
- Fax: **Security policies**
- Phone: Voicemails
- Breach of Confidentiality
- Breach of Privacy

HIPAA Violation and Minimum Civil Penalty

- Reasonable Diligence, (did not know): $100/violation, not to exceed $25,000
- Reasonable Cause: At least $1000/violation, not to exceed $100,000 for each violation
- Willful Neglect, (violation is corrected): About $10,000/violation, not to exceed $250,000
- Willful Neglect, (violation is **not** corrected): $50,000 not to exceed $1,500.000

Criminal Penalties

- Fines (up to $250,000) ,
- Imprisonment (up to 10 years)
- Direct Liability: Covered entity
- "**Corporate Criminal Liability**": Individuals such as directors, employees, officers of the covered entity(organization) can be directly criminally liable under HIPAA.

Reporting

- If 500 or more Consumers' Health Records have been breached, it is a **MUST** to report the breach to the Secretary of the Department of Health and Human Services (HHS) and notify each consumer whose health information has been breached.

- Report privacy breaches to the Privacy Officer.

Recommendations

1. Faxed documents containing protected health information shall be disposed securely upon receipt.
2. Faxed documents shall be routed securely to the appropriate recipient upon receipt.
3. When faxing documents containing PHI within the facility the sender shall alert the receiver of the transmission via phone and/or email.
4. PHI transmitted via email shall be de-identified or encrypted.

Recommendations (Cont.)

5. PHI which happens to be transmitted accidentally via e-mail shall be permanently deleted immediately .
6. Avoid printing documents containing PHI from electronic systems, unless absolutely necessary.
7. Printed documents containing PHI shall be shredded immediately after use.
8. Documents containing PHI shall not be taken home under any circumstances.
9. Computers shall be locked when left unattended
10. IDs and passwords shall not be saved or stored on computers, or sticky notes.

MLJCONSULTANCY LLC

Myson L. Joseph, MHA/INF, RHIA

- Master of Health Administration/Informatics (MHA/INF),

  University Of Phoenix, Online.

  - B.S in Health Information Management,

    Saint Louis University(Doisy College Of Health Sciences)

- Registered Health Information Administrator (RHIA)

Questions?

?

References

- http://www.ahima.org/downloads/pdfs/advocacy/AnalysisofARRAPrivacy-fin-3-2009a.pdf
- http://www.myphr.com/HealthLiteracy/glossary.aspx
- http://www.ahima.org/resources/psc.aspx
- http://www.myphr.com/Privacy/common_privacy_myths.aspx
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- http://journal.ahima.org/2013/01/17/hhs-releases-hipaa-privacy-and-security-update-final-rule/