HIPAA and Gun Control: Software Facilitates This

Due to the restriction imposed by HIPAA, any data concerned with the medical industry can't be used for anything other than treatment unless explicitly signed off for by the patient that the records concern. Now, for any non-treatment related medical research, the files must be de-Identified before transfer from the hospitals database to a third party analysis company. To better understand why de-identification is needed, we must first analyze HIPPA.

What is HIPAA?

HIPAA, or The Health Insurance Portability and Accountability Act, is a set of laws that provide federal protections for individually identifiable health information held by covered entities and their business associates. Since 1996, when the HIPAA was passed by congress, there have been several additions and alterations such as the Health Information Technology for Economic and Clinical Health Act (HITECH ACT) or the more recent Omnibus Final Rule. The final outcome from the HIPAA include but are not limited to:

1. Protection of health coverage for workers and their families when they change or lose jobs
2. The ability to see, copy, and amend your medical records. (Was only available in about half the states)
3. Access to an accounting of anyone who has accessed your medical records in the last six years.
4. The ability to refrain from sharing information about treatment with health providers if paid in full out of the patient's pocket.

Also contained in the HIIPAA is the Privacy Rule, which regulates the use and disclosure of Protected Health Information held by covered entities.

The Privacy Rule

The standards for a covered entity are set in HIPAA. The three classifications they use are Health Care Providers, Health Plans, and Health Care Clearinghouses. Health Care Providers are covered if they transmit any health information electronically. “For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf.”[1] The Health Plan classification includes essentially any company or arrangement that pays for your health care including but not limited to Insurance, HMO’s Medicare, Medicaid, and employee sponsored group health plans. The final classification, health care clearinghouses can be any number of organizations that work as a go-between for health care providers and health plans. [2]

Before the HIPAA Privacy Rule, these entities, unless otherwise forbidden by a state or local law, could pass protected health information to a lender without the patient’s permission. The lender could then deny the patient’s application for a home mortgage or a credit card based on the medical insight. The same scenario could also happen where the protected health information landed in the hands of an employer who uses the information in personnel decisions.

The Privacy Rule has since established basic Federal safeguards to protect the confidentiality of medical information nationwide. Some states have gone above and beyond the Federal privacy standards with stronger protection laws. [3]

The Privacy Rule also lays out some of the exceptions for disclosure of protected health information. One such exemption is when researchers need to recruit for a study. The preparatory research provision permits covered entities to use or disclose protected health information for purposes preparatory to research. However, in this case, the researcher is not allowed to remove protected health information from the covered entity's site. In the case of a researcher who is not a part of a covered entity, a partial waiver of individual authorization could be obtained by an IRB or Privacy Board and give the researcher access to contact information. [4] The other option to receive protected health information is if it has been de-identified or restricted to a limited data set.

De-Identified and Limited Data Sets

If a non-covered entity requires medical records, they will have to receive either de-identified or limited data set records. This means that any information in the record that could link back to the actual patient needs to be redacted. These personal identifiers include:

1. Name
2. Address
3. Date of Birth
4. Phone Numbers
5. Fax Numbers
6. Email Address
7. Social Security Number
8. Medical Record Number
9. Health Insurance Beneficiary #
10. Account Number
11. Certificate Number
12. Vehicle ID (VIN or License Plate)
13. Device ID Number
14. Personal URLs
15. IP Address
16. Biometric ID
17. Facial Images
18. Any Other Unique ID Code

The difference between a de-identified and limited data set record are how many of these fields are required to be pseudonymised. For a de-identified record, all eighteen of these identifiers must be completely anonymized. In the case of limited data sets, only sixteen of the above eighteen are needed, allowing for date of birth and some geographical information such as city, state, or zip code. A limited data set also requires that a data use agreement be signed by whoever is receiving the records.

The Effect on Software

The responsibility of obfuscating the information in these documents ultimately comes down to the responsibility of the software developers who manage medical databases. To comply with the

HIPAA, the software developers must employ advanced algorithms to mask all of the sensitive data. Although not required by law, the masking should always be pre-query masking. Pre-Query masking adds additional security by reducing the risk of internal security breaches. Since nearly half of all security breaches are from losing or misplace corporate assets, it is important to hide the real data even from the hospital workers that will be accessing it. In some cases, the software developers go above and beyond the mandatory restrictions set by HIPAA. For instance, some software allows the records to be backwards masked with the use of an encrypted key. This allows for any results of the research to be used on the patients whose records helped the third party make their discovery.

1. http://www.hhs.gov/ocr/privacy/hipaa/faq/research_disclosures/314.html
2. https://www.privacyrights.org/HIPAA-basics-medical-privacy-electronic-age#3
3. http://privacy.health.ufl.edu/faq/HHS-Facts.shtml#RuleNeed
4. http://www.hhs.gov/ocr/privacy/hipaa/faq/research_disclosures/317.html
5. http://www.beckershospitalreview.com/legal-regulatory-issues/15-things-to-know-about-the-hipaa-omnibus-final-rule-before-sept-23.html
6. http://www.theinformationdaily.com/2012/09/27/75-of-data-breaches-are-inside-jobs
7. https://hipaa.wisc.edu/ResearchGuide/limiteddatasets.html
8. http://en.wikipedia.org/wiki/Hipaa
9. http://www.library.armstrong.edu/eres/docs/eres/MHSA8635-1_CROSBY/8635_week2_HIPAA_politics.pdf
10. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html