POPETH-DPS

September 24, 2020

0.1 Population Health Ethics - Data Privacy and Security (DPS)

There is a constant tension between keeping our data private and the need to collect, store, and use private data to support health sciences decisions making. National databases like NHANES, FluView, MAUDE, and NSSP collect data on individuals' demographic data, disease states, adverse events. They collect data on emergency room visits, reported malfunctions during procedures, and symptoms consistent with influenza (influenza-like illness). To collect data like this, patients/participants allow a certain probability that their data will be compromised and made public—that their identity will be revealed.

The goal of **Data Privacy and Security (DPS)** is to reduce, to as small as possible, the chance a participant's data becomes public knowledge.

In what follows, we'll discuss a definition of privacy, the importance of privacy and HIPAA, the goals of data security and how to ensure your data is secured, approaches to DPS, current challenges in DPS, and a future vision.

0.1.1 Table of Contents:

0.2 Data Privacy

0.2.1 A definition

To quote an excerpt from the book Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research.,

Privacy addresses the question of who has access to personal information and under what conditions. Privacy is concerned with the collection, storage, and use of personal information, and examines whether data can be collected in the first place, as well as the justifications, if any, under which data collected for one purpose can be used for another (secondary)2 purpose. An important issue in privacy analysis is whether the individual has authorized particular uses of his or her personal information (Westin, 1967)

Privacy, in the context of health sciences, is about access. And not only is privacy concerned with **if** we can collect data on individuals but if we **should** collect that data in the first place. To justify collecting data on individuals there should be a proposed benefit to the public or to advancing scientific knowledge that leads to improved well-being in society. Collecting data from individuals puts their privacy at risk and the benefits of collecting data needs to outweigh the risks of a breach of privacy.

0.2.2 Importance of privacy

There are many reasons why privacy is important. But here we discuss reasons why privacy is important to proper data collection.

Ensuring an individuals information is private during data collection reduces the chances of misleading or false information and reduces biases during data collection, leading to a more representative sample of individuals. If an individual suspects data collected from them is likely to not be private, the chances individuals withhold information, or even worse provide false information, increases. This lack of privacy can lead to biased analyses (see this article)—most often response bias, a phenomena where some observations are more probable to be sampled than others.

0.2.3 Common Rule and Informed consent

In part, the Common Rule, or Federal Policy for the Protection of Human Subjects, requires human subjects give informed consent: permission to be included in a research study after the benefits and risks are outlined.

Part of the risks of joining a research study—part of the risks that should be outlined in any informed consent document—is the the risk a subject's privacy is compromised, and if compromised, the potential damage that can be done.

Below is an example statement that outlines the risks to a patient's privacy if they decide to participate in a research study.

Example 01 *The records from this study will be kept as confidential as possible. No individual identities will be used in any reports or publications resulting from the study. All [insert data collection and retention method i.e. questionnaires, tapes, transcripts, summaries] will be given codes and stored separately from any names or other direct identification of participants. Research information will be kept in locked files at all times. Only research personnel will have access to the files and [insert data collection and retention method] and only those with an essential need to see names or other identifying information will have access to that particular file. After the study is completed [state time frame for retaining collect data and whether it will be destroyed].*

Example from recent study To the best of our ability your specific answers in this study will remain confidential. We will minimize any risks by collecting data on a secure server, de-identifying data before analysis, and only presenting aggregate results. To led credence to our results, we do plan on releasing a list with the names and professional affiliations of all respondents. We believe

this is critical to ensuring that the results of this study can be seen as representing a consensus opinion among experts in the field.

0.2.4 HIPPA

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, are set of federal guidelines that determine how patient health information (PHI) can be stored and transmitted. HIPPA is designed to protect patients from having sensitive health information disclosed without asking the patient for consent first. HIPAA is concerned with keeping patient's health data **private**.

HIPPA applied to "covered entities" including: * Healthcare providers * Health plans * Healthcare clearinghouses * Business associates

We'll see that in order to store patient data and also maintain privacy HIPAA also provides guidance on data security.

0.2.5 Lehigh University IRB

It is best to contact **early** Lehigh University's IRB (link here) when working on a research project that involves protected health information or involves collecting data from human subjects.

0.3 Data security

Protected health information (PHI) often links a person's identifying information: name, SSN, health insurance and policy numbers, to all current and past treatments, medications and prescriptions, and diseases they may have. PHI is valuable. With a patient's PHI, criminals can setup false credit cards under a patient's name, request and have filled a patient's prescriptions that they later sell, or hold a patient at ransom, threatening to release private information about that patient to the public.

0.3.1 Goals/Aims and a definition of data security

The goal of data security is to allow only those computers, people, servers, access to data they have been authorized to access. Security ensures those who can read data are the one's allowed to and the aim of data security—in a health sciences setting—is to ensure protected health information is kept private and confidential.

0.3.2 HIPAA security

The HIPAA security rule is a national standard that establishes how to create, store, use, and maintain patient health information. The aim of these security guidelines are to minimize the risk that a patient's records are made public.

From the HIPAA Security rule,

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
3. Protect against reasonably anticipated, impermissible uses or disclosures
4. Ensure compliance by their workforce

and each entity that works with PHI data must consider important aspects of the data they are responsible for such as

1. Its size, complexity, and capabilities,
2. Its technical, hardware, and software infrastructure,
3. The costs of security measures, and

4. The likelihood and possible impact of potential risks to e-PHI.6

0.3.3 HITRUST

Health Information Trust Alliance developed the Common Security Framework is a set of standards that grew from HIPAA, ensuring data security is at the core of data management of PHI. HITRUST can audit a company that stores PHI and if they comply with all HITRUST rules—they recieve a HITRUST certification.

0.3.4 Lehigh University Data Security levels

LU classifies data into four different levels. Level IV is the least restrictive data and level I is the most confidential, restricted data.

Levels: 4. Class IV: Public/Unrestricted Information * Published articles and newsletters, GitHub code, anything public on the web 3. Class III: Institutional/Proprietary Information * Unpublished research data, Vendor non-disclosure agreements 2. Class II: Restricted Information * Student grades, Human Subjects Information 1. Class I: Critical Information * Credit card numbers, SSNs, **PHI**

0.4 When things go bad

0.4.1 Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement

The University of Rochester Medical Center (URMC) has agreed to pay $3 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. URMC includes healthcare components such as the School of Medicine and Dentistry and Strong Memorial Hospital. URMC is one of the largest health systems in New York State with over 26,000 employees.

URMC filed breach reports with OCR in 2013 and 2017 following its discovery that protected health information (PHI) had been impermissibly disclosed through the **loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively**. OCR's investigation revealed that URMC failed to conduct an enterprise-wide risk analysis; implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; utilize device and media controls; and employ a mechanism to encrypt and decrypt electronic protected health information (ePHI) when it was reasonable and appropriate to do so. Of note, in 2010, OCR investigated URMC concerning a similar breach involving a **lost unencrypted flash drive** and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a **lack of encryption** as a high risk to ePHI, URMC permitted the continued use of unencrypted mobile devices.

"Because theft and loss are constant threats, **failing to encrypt mobile devices needlessly puts patient health information at risk**," said Roger Severino, OCR Director. "When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect."

In addition to the monetary settlement, URMC will undertake a corrective action plan that includes two years of monitoring their compliance with the HIPAA Rules. The resolution agreement and corrective action plan may be found at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html.

0.4.2 OCR Settles with 5 Providers Over HIPAA Right of Access Violations

By Jessica Davis

September 15, 2020 - The Office for Civil Rights closed investigations and announced settlements with five providers over separate HIPAA right of access violations, which brings the total number of enforcement actions under its 2019 initiative to seven.

According to the announcement, All Inclusive Medical Services, Beth Israel Lahey Health Behavioral Services, King MD, and Wise Psychiatry have all settled with OCR for failing to adhere to the right of access rule.

Announced in early 2019, OCR's HIPAA right of access initiative strictly enforces the right of patients to obtain access to their medical records in a timely fashion, for a reasonable fee, and in their requested format.

Timely, as studies revealed that more than half of healthcare entities fail to comply with the HIPAA provision. Bayfront Health St. Petersburg in Florida was the first provider to settle with the agency under the initiative for $85,000 in September 2019, followed by Korunda Medical in December 2019.

"Patients can't take charge of their health care decisions, without timely access to their own medical information," OCR Director Roger Severino, said in a statement. "Today's announcement is about empowering patients and holding health care providers accountable for failing to take their HIPAA obligations seriously enough."

0.4.3 Sentara Pays $2.2M for Failing to Properly Report Data Breach to OCR

November 27, 2019 - Sentara Hospitals has settled with the Office for Civil Rights for a $2.175 million civil monetary penalty and a corrective action plan over potential HIPAA violations that include failing to timely and accurately report a data breach to the Department of Health and Human Services.

The health system is made up of 12 acute care hospitals and 300 care sites throughout Virginia and North Carolina.

The settlement centers around a 2017 security incident. OCR received a complaint from an individual who alleged Sentara sent a bill to a patient containing the protected health information of another patient.

The issue is that Sentara reported the incident as only affecting eight patients. Health system officials believed that since the improper disclosure did not contain diagnoses, treatment information, or medical data, that a PHI breach had not occurred.

However, all patient information must be protected under HIPAA. OCR "explicitly advised" Sentara of their reporting duties, but the health system "persisted in its refusal to properly report the breach."

"HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed." OCR Director Roger Severino said in a statement.

0.4.4 Wawa data breach aftermath: Observations from the legal side of things

Back in December 2019, Wawa, Inc. announced that it had "experienced a data security incident" involving malware that had been running on its payment processing systems since as early as March 2019, which "affected payment card information," including credit and debit card numbers and other information." By January 2020, Wawa stated that it had learned of "reports of criminal attempts to sell some customer payment card information potentially involved" in the original data security incident it had reported in December. It expressed its confidence that the malware was contained in mid-December and that only payment card information was involved.

0.5 The current and future of DPS

0.5.1 COVID19 Data Protection Act

0.5.2 Data sharing vs data security

Public Health Surveillance Data: Legal, Policy, Ethical, Regulatory, and Practical Issues

In 2012, the Centers for Disease Control and Prevention (CDC) outlined, as one of their 6 major goals, a goal of improved access to and sharing of data useful for public health surveillance.

The vision All data potentially relevant to public health surveillance would be harmonized across data systems, interoperable, and easily accessed by the maximum number of users in as timely a manner **while protecting confidentiality and privacy of respondents**.

Challenges Constraints on data sharing of nonpublic-use (i.e., restricted) data exist. Occasionally, **(1)** data stewards are reluctant to release data to others because they fear misuse of the data by those who are not well acquainted with its legal and technical limitations on use. In other cases, **(2)** data stewards are not willing to share data either for political or historical reasons or because they fear that if someone else has access to their data their program's importance or visibility might be reduced. However, there are methods that can help protect against the identification of persons. For example, data perturbation is a data security technique that allows users to ascertain key summary information about the data while preventing a security breach.

0.6 Discussion about research and safe storage of data.