# Privacy Risks of Telehealth and Health-Related Applications

By: Maria Auslander

UC Berkeley School of Information

## Introduction

This project aims to assess the privacy risks of sharing health information with applications and the privacy risks associated with telehealth. According to HIPAA journal, about 2.5 million healthcare records were breached through 63 data breaches in October of 2020 (HIPAA Journal, 2020). While most patient data was located in emails and network servers that were breached, personal devices such as laptops, other portable electronic devices, and desktop computers also housed patient health records which were breached.

Beyond health records, which contain the treatment and medical histories of a patient, additional patient health data may inadvertently be shared to third parties through the use of health-related applications, such as those which track insulin levels over time (Blenner et al., 2016). Additionally, the more widespread use of telehealth may lead to more opportunities for patient data breaches, such as the one experienced by Babylon Health (Davis, 2020). Because health-related applications are not covered under HIPAA, unless they're part of a Business Associate Agreement (BAA), they are not subject to additional privacy regulations on the basis of housing health information. In order to better protect the privacy of patients, HIPAA should be appended to include health related applications as covered entities, health applications should update their privacy practices, and health care providers and health-related applications should work to ensure patients are more privacy-aware.

Brief History of Healthcare Data and Current Regulations

## Henrietta Lacks

In 1951, Henrietta Lacks died from cervical cancer. While treating Lacks months before her death, doctors at John Hopkins Hospital had taken samples of her cancerous cells (HeLa cells) to use for research without her consent or knowledge (Nature, 2020). The use of these cells undoubtedly led to wonderful advances in modern medicine, aiding in the development of the polio vaccine, the study of leukemia, and AIDS research, to name a few (Butanis, 2017). However, there are ethical questions that arise from the Lacks case, primarily around informed consent.

While many researchers had prosperous careers due to research conducted on HeLa cells, the Lacks family did not directly benefit from research, and for a long time the positive legacy of Henrietta's cells was unknown to the Lacks. Additionally, in 2013, a team of researchers released the genome sequence of one strain of HeLa cells (Beskow, 2016). While the release of the genome sequence did not break any laws, it was done without the consent of the Lacks family, and the genome sequence provides sensitive biomedical information about Lack's descendants. Following the release of the genome sequence from a strain of HeLa cells, the National Institutes of Health (NIH) reached an agreement with the Lacks family where NIH-funded researchers are required to place information in a database that has controlled access and applications to study the data are reviewed by a committee including the Lacks family (Greely & Cho, 2013).

## Tuskegee Syphilis Experiment

In 1932, the Public Health Service and Tuskegee Institute began work on "Tuskegee Study of Untreated Syphilis in the Negro Male", a study that recorded the natural history of

syphilis in hopes to justify treatment programs for black Americans (CDC, 2020). The experiment was originally conducted on 600 black men without their consent, this included 399 men who had syphilis and 201 men who did not have syphilis. While researchers told the men they were being treated for "bad blood", the men did not actually receive appropriate treatment to cure their illness. Men were compensated in the form of free medical exams, free meals, and burial insurance rather than treatment for the disease.

While originally expected to last 6 months, the study lasted 40 years, ending in 1972 when news articles began to condemn the study. In 1974 an out-of-court settlement was reached to give medical benefits to the men who were part of the study (through the Tuskegee Health Benefit Program). In addition to the benefits program, the National Research Act gained traction in 1974 following the notoriety of the Tuskegee Syphilis Experiment. The Belmont Report was released by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research as a result of the National Research Act of 1974, the report brings to light ethical considerations around subject's rights (1978).

Belmont Report

The Belmont Report was written in response to the National Research Act of 1974. The report lays out three ethical principles with respect to subject rights, including Respect for Persons, Beneficence, and Justice (1978).

The **Respect for Persons** principle states that individuals should be treated as autonomous agents and persons with diminished autonomy are entitled to protections. The importance of informed consent is underscored with the Respect for Persons principle. In recognizing that autonomy needs to be respected, the principle states that individuals need to voluntarily participate in research after being made aware of any potential harms or benefits that

may result from a study they are participating in. In the case of the Tuskegee study, the Respect for Persons principle was not met as individuals were not treated as autonomous agents who were at liberty to make the decision of whether or not to participate in the study.

The **Beneficence** principle states that individuals should be treated in an ethical way that not only reduces harms to individuals, but additionally maximizes benefits to individuals participating in research. In medical studies, it is inferred that treatment is to be provided to individuals who are suffering from an ailment as part of their participation in research. In the Tuskegee study, this principle was not respected as while individuals were given medical exams, they were not treated for Syphilis.

The **Justice** principle asks the question of "Who ought to receive the benefits of research and bear its burdens?". This is to preface the argument that the distribution of benefits of research and burdens of research should be fairly distributed. In the case of the Tuskegee study, the participants were not treated with Justice as they were unfairly denied treatment for Syphilis.

While the Belmont Report provides valuable instructive information for researchers who study information with respect to human subjects, its applicability in the 21st century has been questioned. For example, in some cases there is potentially valuable future research that could be conducted using biospecimens, but there is no clear indicator of how consent should be obtained for future studies using the same biospecimens (Brothers et al., 2019). Following the Belmont Report, HIPAA was passed to protect the flow of healthcare information.

## HIPAA

The Healthcare Insurance Portability and Accountability Act (HIPAA) was passed in 1996 partially to regulate the flow of healthcare information and safeguard protected health information (PHI) from theft or from fraudulent use through its Privacy Rule (HHS, 2020). The

Privacy Rule is a Federal law that gives Americans rights over their health information and provides limits on who can receive PHI, the rule applies to all forms of PHI, including electronic, written, and oral data. The Privacy Rule limits the flow of health information by setting boundaries on the release of the health records, giving patients more control over their information, and by establishing safeguards that health care providers need to achieve to protect patient information. HIPAA is maintained by the U.S. Department of Health & Human Services (HHS). General information is readily available on the HHS website (HHS.gov), but specific measures taken with respect to HIPAA are less readily available (i.e. the means through which boundaries are set on the release of health records).

HIPAA regulations apply to covered entities, covered entities include health care providers, health plans, and health care clearinghouses (HHS, 2017). Additionally, covered entities are required to maintain contracts with any business entities that may help carry out healthcare-related activities through Business Associate Agreements (BAAs). Health-related applications are not subject to HIPAA regulations unless they have a BAA with a covered entity. Definitions of covered entities are in appendix A2.

The increasing use of information technology in healthcare has led to many suggestions to update HIPAA accordingly (Harrod, 2019). Since it was enacted in 1996, there have been several updates to HIPAA to enable better patient privacy. These updates have included the mandate to release reports concerning health record breaches and the Final Omnibus Rule which relates to encryption standards. A helpful visual showing the brief timeline of events since HIPAA was enacted is below:

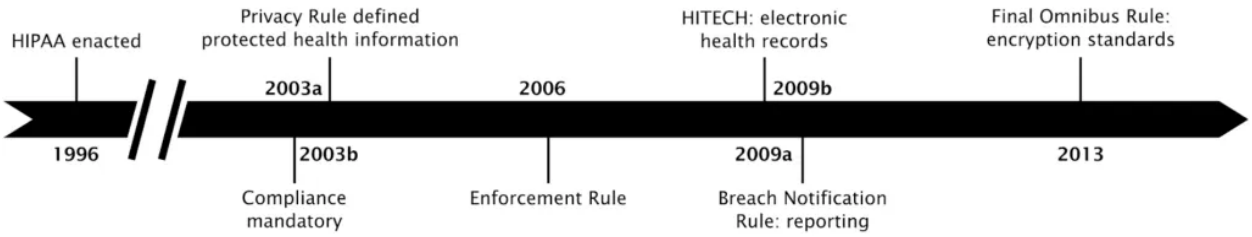


*Figure 1: History of US health data privacy law. (Harrod, 2019)*

## Telehealth and Privacy

Telehealth is the use of electronic information and telecommunication technologies to provide care when a patient and his or her provider aren't in the same place at the same time (HHS, 2020). Telehealth allows patients to communicate with their providers outside of a medical setting and also allows for remote patient monitoring. Telehealth can be largely beneficial to both patients and providers with respect to convenience. Patients who live in rural areas can receive lab work closer to home, but still receive the guidance of top health care providers throughout the United States. Individuals who may rely on public transportation in large cities who may put themselves at risk by using public transportation during a global pandemic can communicate with providers in the relative safety of their homes. However, telehealth can pose privacy risks.

Telehealth has become increasingly popular throughout the COVID-19 pandemic. According to Insider Intelligence, in March 2020, 53% of providers surveyed found they "now use telemedicine because of the restrictions imposed by COVID-19, but have not used telemedicine prior to the pandemic" (more detail is shown in figure 2) (Han, 2020) . This is a notable surge in the popularity of telehealth, additionally, the American Telemedicine Association (ATA) iprojects "more than 50% of health care services will be consumed virtually by 2030", though this may be a biased source (ATA, 2019).

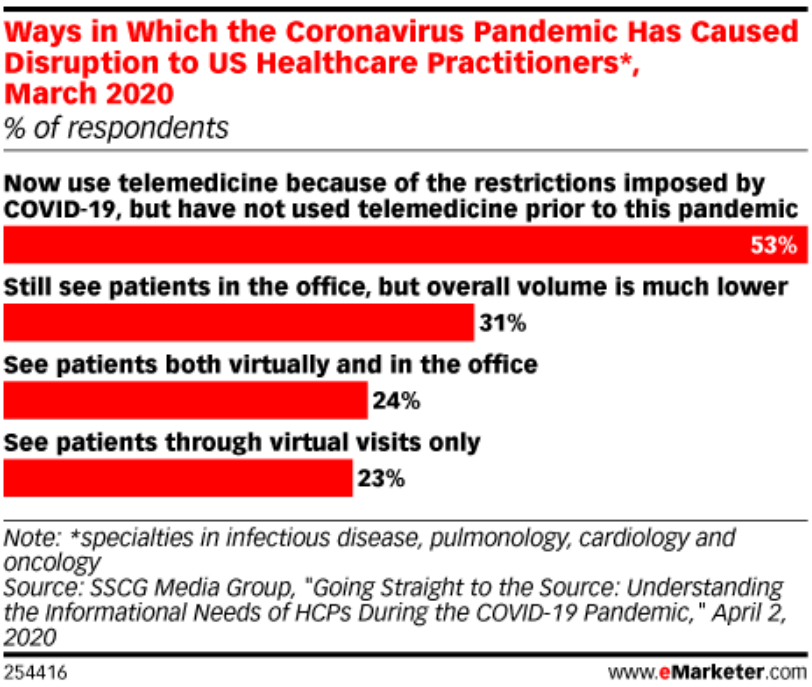


*Figure 2: Ways in Which the Coronavirus Pandemic Has Cause Disruption (Han, 2020)*

The COVID-19 pandemic has led to more lenient regulations with respect to the disclosure of health information as it pertains to telehealth. The Office for Civil Rights (OCR) at HHS has elected to exercise enforcement discretion and will not impose penalties against health care providers who may not follow HIPAA guidelines in choosing telecommunication providers for telehealth services. This is in connection with the good faith provision of telehealth during the global COVID-19 pandemic (HHS, 2020). Following the COVID-19 pandemic, privacy concerns resulting from telehealth practices may be more easily addressed.

An aspect of telehealth is telemonitoring, which "is defined as the use of information technology to monitor patients at a distance" (Meystre, 2005). Telemonitoring allows patients to share relevant information with providers that may aid in the state of their health. For example, telemonitoring has been helpful in the space of heart failure management, reducing all-cause mortality and chronic heart failure related hospitalizations (Inglis et al., 2010). However,

telemonitoring carries privacy risk if relevant data is intentionally or unintentionally shared with inappropriate entities.

While health care providers are tasked with protecting patient data through HIPAA, there are many entities that may collect health-related information that are not subject to regulation through HIPAA. One example is Facebook's Preventative Health tool, which is not covered as HIPAA does not extend to information shared on social media platforms or health related applications, unless the applications have a BAA with a covered entity (Bari & O'Neill, 2019). While Facebook has stated that health information will not be publicly available or shared with third parties, individuals who work on the product will have access (Facebook, 2019). More detail on Facebook's Preventative Health tool is available in Appendix A3. In addition to the increased popularity of telehealth, the lack of regulation for health data collected through social media platforms and applications may present a case to modernize HIPAA.

Telehealth with Respect to Privacy Frameworks

When assessing the privacy risks associated with telehealth, it's important to consider the risks through well laid out logical frameworks. Below, the privacy risks associated with telehealth will be addressed through the lens of Solove's Taxonomy of Privacy, Nissenbaum's Contextual Integrity, and Mulligan et al.'s Analytic. Further detail on the definitions of terms laid out through the privacy frameworks listed is in Appendix A1.

*Solove's Taxonomy of Privacy*

Solove's Taxonomy assesses privacy risk through the lens of the **data subject**, **information collection**, **information processing**, **data holders**, **information dissemination**, and privacy **invasions** (Solove, 2006). With respect to telehealth, the data subject is the patient

whose medical information is collected through both **surveillance** (i.e. recording of a patient visit) and **interrogation** (i.e. targeted questions by health care providers that may relate to a diagnosis). Health information is often maintained and processed by Electronic Medical Record (EMR) services such as Epic Systems which maintains the health records of over 250 million patients (Epic). Epic and other EMR companies work with health care systems to aggregate patient information and in some cases share this information with third parties. In some cases healthcare information is breached. For example, in October 2020, there were 63 reported breaches of 500 or more records, where a total of over 2.5 million individuals had their health data exposed (HIPAA Journal, 2020). The majority of breached patient data was located in email or in network servers.

*Nissenbaum's Contextual Approach to Privacy Online*

According to Nissenbaum's Contextual Approach to Privacy Online, the key parameters of informational norms are **actors**, **attributes**, and **transmission principles** (Nissenbaum, 2011). Actors consist of subjects, senders, or recipients. Attributes consist of types of information. Transmission principles refer to the constraints under which information flows. Under Nissenbaum's approach, personal information privacy is grounded in two norms—'appropriateness' and 'distribution' (or 'flow')—that Nissenbaum argues are individually necessary and jointly sufficient for privacy. According to Nissenbaum, the context under which information flows is important.

In the context of COVID-19, the restrictions under which patient information flows with respect to telehealth has been reduced. As previously mentioned, the HHS has determined that it is appropriate to limit the restrictions on telehealth as the need for telehealth has increased during the global COVID-19 pandemic. However, due to the sensitive nature of health information, it

would be reasonable to expect that HIPAA regulation restrictions on telehealth will be better maintained following the coronavirus pandemic. Additionally, the HHS has provided additional information with respect to the good faith provision that allows for lessened restrictions during the COVID-19 pandemic, stating that certain actions are not protected under the good faith provision granted due to the pandemic. These actions include context that may indicate a criminal act, such as fraud, and disclosures of patient data that are prohibited by the HIPAA Privacy Rule such as the sale of data or the use of data for marketing (HHS, 2020).

*Mulligan et al.'s Multidimensional Analytic for Mapping Privacy*

Stating that privacy is an essentially contested concept, Mulligan et al. provide a useful multi-dimensional analytic for mapping privacy. The 14 dimensions of privacy laid out by the analytic are: **object, justification, exemplar, contrast concept, exemplar, target, subject, action, offender, from-whom, mechanism, provider, social boundaries, temporal scale, and quantitative scope** (Mulligan et al., 2016). These dimensions are defined in appendix A1. Examples of how the dimensions of the analytic are related to privacy issues around health data are below:

| **Dimension** | **Example** |
|---|---|
| Object | Privacy provides patients with a sense of security over their health data |
| Justification | Health data should be private as knowing health-related information about an individual may change one's perception of said individual |
| Contrast Concept | Contrasting to privacy, health data would not be private if it was publicly released |
| Exemplar | Privacy is threatened through dissemination of health data, through database invasions and through unintentional releases of data |
| Target | Privacy protects patients, patients can be the targets of malicious actors |
| Subject | Data is related to patients, patients are the subjects |

| Dimension | Example |
|---|---|
| Action | The action of hacking a health related database or the act of inadvertently release health information would cause harm |
| Offender | Privacy could potentially be violated by offenders such as hackers who gain access to health information |
| From-Whom | Privacy protects patients from hackers and others who may use their data inappropriately |
| Mechanism | Encryption of data in transit is a mechanism to protect patient privacy |
| Provider | According to HIPAA, covered entities are charged with providing privacy to patient information. Other entities that hold patient data, such as health-related applications, should also be held accountable. |
| Social Boundaries | Privacy rules apply to health care providers, currently social media applications are not charged explicitly to protect health information outside of typical health records |
| Temporal Scale | Health data should be protected throughout a patient's life and beyond |
| Quantitative Scope | Privacy surrounding health-related data should be wide reaching. Inappropriate actors (hackers, third party applications, etc.) should not be able to access health data from HIPAA covered entities or health related applications |

Case Study I: Apple Health

Apple is a tech giant that has utilized the collection of health data to offer users different features. While imperfect, unlike Facebook, Apple's advertising platform does not share personally identifiable information with third parties (Apple, 2020). Therefore, Apple may be better suited than some other tech giants to gain the trust of consumers when it comes to health related tools. While Apple may be in a better position to handle health-related data, the data they do collect and use is arguably more comprehensive and sensitive than the data collected as part other health tools such as Facebook's Preventative Health.

Apple Health consolidates health data from users' smartphones, smart watches, and third party apps and allows users to view health-related metrics (Apple ). Apple Health automatically

collects and aggregates data such as steps, walking and running distances, and allows users to house information from other applications such as heart rate data from Apple Watches. These data points could help determine the state of one's health in some way (i.e. someone with an irregular heartbeat may have heart disease, those with a low amount of steps could lead sedentary lifestyles, etc). Given that knowing the state of someone's health could change one's perception of that individual, maintaining privacy for health related data is of pivotal importance.

In addition to collecting data from third party applications, Apple states that third party applications which use Apple Health are required to have a privacy policy (Apple). However, Apple does not provide detail on stipulations that need to be laid out by said privacy policies. If Apple does not provide relevant detail to third parties on what needs to be contained in their privacy policies, this indicates a third party application using Apple Health data could have a statement in their privacy policy which allows them to share data with other third party applications and user data could be inappropriately transmitted.

In addition to providing information such as steps walked per day, etc. Apple Health also allows users to view health records from participating health institutions. Health records include information such as clinical vitals, conditions, and lab results. Apple claims that users are in charge of their health data, stating that users decide which information is placed in Apple Health and which apps can access data through the Health app. Additionally, Apple encrypts health data when iPhones are locked. While measures have been put in place to protect patient privacy, it is notable that Apple has avoided responsibility in terms of HIPAA compliance through the development of this feature. This is clear in the language of the statement "As part of this feature, Apple is not creating, receiving, maintaining, or transmitting protected health information for or on behalf of a covered entity or business associate" (Apple, 2020).

## Case Study II: Babylon Health Breach

In June of 2020, those vying for public trust in telehealth methods suffered a blow when Babylon Health when a patient found he was able to view videos from other patients' appointments in the Babylon Health application (Davis, 2020). Babylon said this disclosure of information occurred due to a software error that occurred through the release of a new feature, and not through a malicious attack or invasion. Regardless of how the disclosure occurred, it raises privacy concerns. Additionally, if an application user could access other users' information, it would not be too much of a stretch to assume that cybercriminals may also be able to access valuable patient information stored in the application as well.

While the Babylon incident occurred in the UK, the breach brings concerns around the privacy risks of telehealth to the surface globally. Patients are eager to protect their health information and reduce potential harms to themselves. Revealing health information could affect how other individuals perceive an individual, negative judgement may come to those who have certain health conditions or who have had certain medical procedures. For example, judgement is often passed to women who get abortions, these women would likely not want their health history to be public, and abortion clinics have been subjected to increasing cyberattacks (Grant, 2017). Beyond negative judgement from individuals, patients may be concerned if insurance companies were able to view information concerning their health, affecting their premiums.

## Suggestions

Telehealth and the broad use of mobile technologies for healthcare have mandated updates to the current treatment of patient data in terms of privacy. Suggestions include updates to HIPAA to include more provisions around telehealth and restrictions on social media sites,

updating privacy practices for health-related applications, and a push for more privacy aware patients. Suggestions are detailed in the subsections below.

Updates to HIPAA in a post-COVID-19 World

While there have been pertinent updates to HIPAA since it was initially passed, there are still many ways in which health information is not protected through the act. A striking weak point of HIPAA is it's failure to protect individuals from privacy risks that are conceived by non-covered entities. As previously stated, covered entities include health care providers, health plans, and health care clearinghouses (HHS, 2017).

Health-related applications or social media based applications are not included as covered entities with respect to HIPAA, and are not subject to regulations unless they receive PHI from existing covered entities and have signed a BAA. It would be to the benefit of individuals in terms of privacy protection to include health-related applications that do not interact with current covered entities to the list of HIPAA covered entities. One could argue that companies and applications are already subject to regulations from the Federal Trade Commission (FTC), however, the additional privacy risks associated with PHI warrant additional, focused attention.

In addition to adding health-related applications and services to the list of covered entities under HIPAA, following the global COVID-19 pandemic, telehealth services should be subject to regulation from HIPAA as they were preceding the pandemic when it is appropriate to do so. There should be a balance of maintaining patient care and patient privacy through the use of telehealth.

Updating Privacy Practices for Health-Related Applications

While adding health-related applications to the list of covered entities under HIPAA would push companies maintaining these applications to protect user data, applications should take the initiative to protect user data themselves. In many cases, data is shared to third party applications, posing a privacy risk. Additionally, some health-related applications do not have comprehensive privacy policies. For example, a study released in 2016 found that "diabetes apps shared information with third parties" and 81% of 211 diabetes android apps surveyed did not have privacy policies (Blenner et al., 2016). However, it's notable that this study was done prior to the passing of CCPA in 2018, an act intended to enhance privacy rights for California citizens, and CCPA has led to more privacy policies being enacted for companies that do business in California (California Office of the Attorney General, 2020).

Privacy policies inform users of privacy practices at an organization and allow users to know what information is being collected through the use of the application, how the data will be used, and who the data will be visible by. Users have the right to know who will be accessing their health information and what it will be used for. Privacy policies should be written in clear language and should be read by users before they use an application in order to have a form of informed consent for health application users. Within the policy, practices around data security should be ensured and described. Health related applications should not share user health information with any third parties, unless it is appropriate; for example, an app may send information to a user's health care provider. Clear privacy practices, and the protection of data from inappropriate invasions or inappropriate dissemination will increase trust in health-related applications, benefiting both the companies owning the applications and their users.

Privacy-Aware Patients

Beyond the use of privacy policies and adherence to HIPAA, health care systems, health care providers, and health-related applications should encourage users to be aware of privacy concerns and their rights. Health care providers and systems may be able to inform patients of ways they can maintain privacy while participating in telehealth while practicing in a way that is conducive to patient privacy. For example, health care systems may encourage the use of HIPAA-approved telehealth platforms such as Updox and  provide instructions on how patients can use these platforms with their health care providers. Health care systems could also advise patients to participate in telehealth visits on private devices when possible. Health-related applications could provide concise privacy information to users as they use the application initially. For example, as an application collects information about the user, the application could also give the user information on how the information being collected by the application is being protected and what the data is being used for.

## Conclusion

This discussion has been centered around the privacy implications of telehealth or the use of technologies which collect health related information. Past privacy indiscretions such as those exemplified by the case of Henrietta Lacks and the Tuskegee Syphilis Experiment have informed protections of patients participating in health research. HIPAA was released in 1996 to protect patient information. While valuable work has been done to protect patients through current regulations, policies could be improved to protect patients as health technology advances. Telehealth has become increasingly popular in recent years, with a surge of telehealth visits occurring in 2020 due to the global coronavirus pandemic. While telehealth is hugely beneficial in connecting patients with providers, there privacy issues related to the delivery of telehealth. In

one example, the Babylon Health app inadvertently released patient data to other patients. Health care systems and providers, as well as companies owning health-related applications should make it a top priority to protect patient privacy when providing patients with remote care. This will increase patient trust in telehealth, benefitting all involved in the patient process.

References

Apple. (2020). *Healthcare - Health Records*. Apple. https://www.apple.com/healthcare/health-records/.

Apple. (2020, September 18). *Apple Advertising & Privacy*. Apple Support. https://support.apple.com/en-us/HT205223.

ATA. (2019). *ATA Action Briefs*. Health Care Consumerization. https://info.americantelemed.org/ata-action-briefs_healthcare-consumerization.

Bari, L., & O'Neill, D. P. (2019, December 12). Rethinking Patient Data Privacy In The Era Of Digital Health [web log]. https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full/.

Beskow, L. M. (2016, August 31). *Lessons from HeLa Cells: The Ethics and Policy of Biospecimens*. Annual review of genomics and human genetics. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5072843/.

Blenner, S. R., Köllmer, M., Rouse, A. J., Daneshvar, N., Williams, C., & Andrews, L. B. (2016). Privacy Policies of Android Diabetes Apps and Sharing of Health Information. *Jama*, *315*(10), 1051. https://doi.org/10.1001/jama.2015.19426

Brothers, K. B., Rivera, S. M., Cadigan, R. J., Sharp, R. R., & Goldenberg, A. J. (2019). A Belmont Reboot: Building a Normative Foundation for Human Research in the 21st Century. *The Journal of Law, Medicine & Ethics*, *47*(1), 165–172. https://doi.org/10.1177/1073110519840497

Butanis, B. (2017, April 11). *The Importance of HeLa Cells*. Johns Hopkins Medicine. https://www.hopkinsmedicine.org/henriettalacks/importance-of-hela-cells.html.

*California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of

the Attorney General. (2020, July 20). https://oag.ca.gov/privacy/ccpa.

Centers for Disease Control and Prevention. (2020, March 2). *Tuskegee Study - Timeline - CDC - NCHHSTP*. Centers for Disease Control and Prevention. https://www.cdc.gov/tuskegee/timeline.htm.

Davis, J. (2020, June 11). *Breach of Telehealth App Babylon Health Raises Privacy Concerns*. HealthITSecurity. https://healthitsecurity.com/news/breach-of-telehealth-app-babylon-health-raises-privacy-concerns.

Epic. *About Us*. Epic. https://www.epic.com/about.

FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. (2019, July 24). *Federal Trade Commission*. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

Grant, R. (2017, May 10). *Cyberattacks Against Abortion Clinics Have Increased At an Alarming Rate*. Wired. https://www.wired.com/story/cyberattacks-against-abortion-clinics/.

Greely, H. T., & Cho, M. K. (2013, October). *The Henrietta Lacks legacy grows*. EMBO reports. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3807222.

Han, J. (2020, April 13). *Telemedicine Could Be More Widely Adopted Due to the Coronavirus*. Insider Intelligence. https://www.emarketer.com/content/telemedicine-could-be-more-widely-adopted-due-to-the-coronavirus.

Harrod, J. (2019, May 16). *Health Data Privacy: Updating HIPAA to match today's technology*

*challenges*. Science in the News. http://sitn.hms.harvard.edu/flash/2019/health-data-privacy/.

Henrietta Lacks: science must right a historical wrong. (2020). *Nature*, *585*(7823), 7–7. https://doi.org/10.1038/d41586-020-02494-z

HHS. (2015, November 23). *Health Care Clearinghouse.* HHS. https://aspe.hhs.gov/report/standards-privacy-individually-identifiable-health-information-final-privacy-rule-preamble/health-care-clearinghouse.

HHS. (2020, April 10). *3023-What may constitute bad faith in the provision of telehealth by a covered health care provider, which would not be covered by the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications?* HHS.gov. https://www.hhs.gov/hipaa/for-professionals/faq/3023/what-may-constitute-bad-faith-in-tHe-provision-of-telehealth-by-a-covered-health-care-provider-which-would-not-be-covered-by-the-notification-of-enforcement-discretion-regarding-covid-19-and-remote-telehealth/index.html.

Inglis, S. C., Clark, R. A., Mcalister, F. A., Ball, J., Lewinter, C., Cullington, D., … Cleland, J. G. (2010). Structured telephone support or telemonitoring programmes for patients with chronic heart failure. *Cochrane Database of Systematic Reviews*. https://doi.org/10.1002/14651858.cd007228.pub2

*iOS - Health*. Apple. https://www.apple.com/ios/health/.

Meystre, S. (2005). The Current State of Telemonitoring: A Comment on the Literature. *Telemedicine and e-Health*, *11*(1), 63–69. https://doi.org/10.1089/tmj.2005.11.63

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a

multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont report: ethical principles and guidelines for the protection of human subjects of research*. The Commission.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/daed_a_00113

*October 2020 Healthcare Data Breach Report*. HIPAA Journal. (2020, December 3). https://www.hipaajournal.com/october-2020-healthcare-data-breach-report/.

*Privacy Matters: Facebook's Preventive Health Tool*. About Facebook. (2019, October 28). https://about.fb.com/news/2019/10/privacy-matters-preventive-health/.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

*Understanding telehealth*. Telehealth.HHS.gov. (2020). https://telehealth.hhs.gov/patients/understanding-telehealth/?gclid=CjwKCAiA5IL-BRAzEiwA0lcWYrjjzgS_AV_O2nDJHyq4M2mWMkcj0EvwY8gmdAOnCPiB311MozTfRxoCyCcQAvD_BwE.

US Department of Health and Human Services. (2017, June 16). *Covered Entities and Business Associates*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

US Department of Health and Human Services. (2020, March 30). *Notification of Enforcement Discretion for Telehealth*. HHS.gov.

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

US Department of Health and Human Services. (2020, November 2). *Your Rights Under HIPAA*. HHS.gov. https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

*What is Preventive Health on Facebook?* Facebook. (2019). https://www.facebook.com/help/iphone-app/279392126259317?helpref=platform_switcher.

Appendix

A1: Definitions and Origins of Terms (Privacy Frameworks)

The following table provides additional detail around terms used throughout the discussion with respect to privacy frameworks. The terms have been taken from Solove's "A Taxonomy of Privacy" (2006), Nissenbaum's "A Contextual Approach to Privacy Online" (2011), and Mulligan et al.'s multidimensional analytic for mapping privacy (2016).

| **Term** | **Definition** | **Origin** |
|---|---|---|
| Data Subject | The individual whose life is most directly affected by data-related activities | Solove |
| Surveillance | The watching, listening to, or recording of an individual's activities | Solove |
| Interrogation | Various forms of questioning or probing for information | Solove |
| Aggregation | The combination of various pieces of data about a person. | Solove |
| Identification | Linking information to particular individuals. | Solove |
| Insecurity | Carelessness in protecting stored information from leaks and improper access | Solove |
| Secondary Use | The use of information collected for one purpose for a different purpose without the data subject's consent | Solove |
| Exclusion | The failure to allow the data subject to know about the data that others have about her and participate in its handling and use. | Solove |
| Breach of confidentiality | Is breaking a promise to keep a person's information confidential | Solove |
| Disclosure | The revelation of truthful information about a person that impacts the way others judge her character | Solove |

| Term | Definition | Origin |
|---|---|---|
| Exposure | Revealing another's nudity, grief, or bodily functions | Solove |
| Increased Accessibility | Amplifying the accessibility of information | Solove |
| Blackmail | The threat to disclose personal information | Solove |
| Appropriation | The use of the data subject's identity to serve the aims and interests of another | Solove |
| Distortion | The dissemination of false or misleading information about individuals | Solove |
| Intrusion | Invasive acts that disturb one's tranquility or solitude | Solove |
| Decisional Interference | The government's incursion into the data subject's decisions regarding her private affairs | Solove |
| Actors | Subjects, senders, and recipients of data | Nissenbaum |
| Subject (Nissenbaum) | Individual who data/information is related to | Nissenbaum |
| Sender | Entity involved in the distribution of information | Nissenbaum |
| Recipient | Entity who receives subject information | Nissenbaum |
| Attributes | Types of information | Nissenbaum |
| Transmission Principles | Constraints under which information flows | Nissenbaum |
| Object | That which privacy provides to those protected, i.e. privacy provides protected agents with X | Mulligan |
| Justification | The motivation and basis for providing privacy, i.e. privacy is justified because of X | Mulligan |
| Contrast Concept | That which contrasts to privacy, i.e. that which is private is mutually exclusive with that which is X | Mulligan |
| Exemplar | The archetypal threat to this concept of privacy, i.e. privacy is violated by X | Mulligan |
| Target | That which privacy protects, i.e. privacy protects things of type X | Mulligan |

| Term | Definition | Origin |
|---|---|---|
| Subject (Mulligan) | Actor(s) or entity(ies) protected by privacy, i.e. privacy protects agent X | Mulligan |
| Action | The act or behaviour that initiates or constitutes a privacy harm | Mulligan |
| Offender | Actor(s) violating privacy, i.e. privacy violated by agent X | Mulligan |
| From-Whom | Actor(s) against-whom privacy is a protection, i.e. privacy provides protection against agent X | Mulligan |
| Mechanism | That which instrumentally secures privacy, i.e. the lock on her door protected her privacy | Mulligan |
| Provider | Actor(s) charged with securing privacy, i.e. the telecommunications provider was responsible for technically securing the privacy of her communications | Mulligan |
| Social Boundaries | That wherein privacy applies, i.e. privacy applies in domain, situation, field, or site X | Mulligan |
| Temporal Scale | The time span at which privacy applies, i.e. privacy applies for a span of X time | Mulligan |
| Quantitative Scope | Extent of application of privacy, i.e. privacy should be applied with a scope of X | Mulligan |

A2: Definitions of HIPAA Covered Entities

| A Health Care Provider | A Health Plan | A Health Care Clearinghouse |
|---|---|---|
| This includes providers such as:<br>• Doctors<br>• Clinics<br>• Psychologists<br>• Dentists<br>• Chiropractors<br>• Nursing Homes<br>• Pharmacies<br>...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard. | This includes:<br>• Health insurance companies<br>• HMOs<br>• Company health plans<br>• Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs | This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa. |

Covered Entity Definitions. (Image from HHS)

While the definition of a “Health Care Clearinghouse” is vague, examples given for Health Care Clearinghouses as provided by the US Department of Health & Human Services are “Billing services, repricing companies, community health management information systems, community health information systems, and "value-added" networks” (HHS, 2015).

A3: Facebook's Preventative Health Tool

In 2019, Facebook released a tool called "Preventative Health" that allows users to see health checkups which are meant to help users prevent disease and stay healthy (Facebook, 2019). The tool relies on information like personal health and family history. The tool also uses the user's location in order to show nearby health checkup locations. Information gained through Preventative Health will not intentionally be shared with third parties. However, Facebook does mention that actions related to the use of the Preventative Health tool could be shared with third parties, for example, "liking the Facebook page of a health organization or visiting an external website linked to from Preventive Health" (Facebook, 2019).

While Facebook does appear to value health data from the privacy standpoint more than other data they may share with third parties for advertising, users should be aware that information gained through social media platforms is not protected by HIPAA. The use of a preventative health tool embedded within a widely used social media platform could be doubtlessly useful; but this lack of protection from HIPAA means users are putting the privacy of their health data in the hands of Facebook, a company with a track record of past privacy indiscretions which led to a $5 billion FTC settlement (FTC, 2019).