Project Nightingale - The Case for Increased Privacy
By Elizabeth Magnan[1]

In an increasingly connected world, where technology companies are gathering private and personal information on millions of Americans, it is important to protect the personal health information of each individual. Technology companies like Google, Amazon, and Apple are progressively moving into the healthcare industry through patient's medical records.[2] On November 11, 2019, Google announced that since July 2019 they had been partnering with Ascension, one of the nation's leading non-profit health systems, to assist them in creating better technology to support care for their patients, through sharing patient medical records.[3] Ascension is transferring the medical records of millions of patients to Google as part of a massive shift to cloud infrastructure and storage of medical records.[4] Along with providing cloud infrastructure, the partnership also includes the transfer of patient medical records for Google to use in new Machine learning and advanced Artificial Intelligence (AI) programs.[5]

The data involved includes lab results, diagnoses and hospitalization records, which can amount to a complete health history along with patient names and dates of birth.[6] This project, also known as "Project Nightingale," is an attempt to use the health information of millions of individuals to create AI and machine learning tools to predict patterns of illness that could lead to new treatments or cures.[7] This is surely an admirable goal, but neither doctors nor patients were notified that their records were being transferred to the tech giant.[8] In a world that is acutely aware of and concerned with data security breaches, and where consumers demand to know how their data is being used, it is concerning that both Google and Ascension decided to keep this partnership a secret.

Transparency about the use and transfer of our data has become one of the main issues in privacy laws and considerations around the world. The fact that Google hid the transfer of health care records of millions of patients is unsettling. Under HIPAA, hospitals and healthcare organizations are generally allowed to share data with business partners without telling patients, as long as that information is used to help covered entities carry out their health care functions.[9] "A 'business entity' is an entity that performs certain functions or activities that involve the use or disclosure of 'protected health information' on behalf of, or provides certain services to, a covered entity that is not a member of the covered entity's workforce."[10] While Ascension and Google are not strictly required to disclose their business relationship or the transfer of records under HIPAA, they should have. Whether Google was only providing cloud services for medical records is a separate conversation, but the fact that Ascension is transferring medical records of patients to the tech giant to use in their AI programs, and granting over 150 Google employees

---

[1] Elizabeth Magnan graduated from Santa Clara University in spring 2020. This paper was written as a requirement for the privacy certificate, in conjunction with the article written by Monica Tapavalu.

[2] Rob Copeland, *Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans,* THE WALL STREET JOURNAL (Nov. 11, 2019), https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

[3] Tariq Shaukat, *Our partnership with Ascension,* GOOGLE CLOUD (Nov. 11, 2019), https://cloud.google.com/blog/topics/inside-google-cloud/our-partnership-with-ascension.

[4] *Id*.

[5] Rob Copeland, *Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans,* THE WALL STREET JOURNAL (Nov. 11, 2019), https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

[6] *Id*.

[7] *I'm the Google whistleblower. The medical data of millions of Americans is at risk,* THE GUARDIAN (Nov. 14, 2019) https://www.theguardian.com/commentisfree/2019/nov/14/im-the-google-whistleblower-the-medical-data-of-millions-of-americans-is-at-risk.

[8] Copeland, *supra* note 4.

[9] *Id*.

[10] Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI & TECH. L. REV. 429, 433 (2015).

complete access to all the records in secret, is worrying for privacy-focused individuals.[11] Furthermore, Ascension and Google only disclosed details of the arrangement after an article was published in the Wall Street Journal.[12] It is hard to trust the assurances of companies, like Google, that they are only using the data in the patient's best interest, when their first instinct is to be secretive about the transfer and use of that data.

The HIPAA Privacy rule requires that business associates provide assurances to health plans that they will only use the health information provided to them for the purposes it was solicited for by the covered entity.[13] This includes the requirement that they will safeguard the information from misuse.[14] Most importantly, "[c]overed entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate."[15] While this might normally limit what Google can do with the data, the broadness of their stated goals makes it difficult to find an actual limitation.

HIPAA allows for flexible and individually designed contracts between covered entities and their service providers in the form of Business Associate Agreements.[16] One of the goals included within the Google-Ascension partnership is "[e]xploring artificial intelligence/machine learning applications that will have the potential to support improvements in clinical quality and effectiveness, patient safety, and advocacy on behalf of vulnerable populations, as well as increase consumer and provider satisfaction."[17] This is a commendable goal, and in a world of big data, an important task.

With the spread of COVID-19 around the world today, it is easy to see the benefits of big data and machine learning to fight these diseases and pandemics. However, once the data is transferred and incorporated within these systems, it is almost impossible to retract. It is easy to look at big data or precision public health studies that work to predict patterns or spreads of diseases and see the benefits.[18] These studies are important and are a way to improve medicine as well as identify at risk populations. Yet, these gains must be weighed against the rights of the individual. There are numerous ways that big data and privacy can intermix through de-identification, hashing, and aggregation that would allow for the continuation of these benefits while still protecting the privacy of the individual.

HIPAA is designed to protect patient health information, and while it does allow business associates to gain access to and use health care information to assist covered entities in their business, there is also a minimum necessary standard. The minimum necessary standard comes from the HIPAA Privacy Rule.[19] "Under the HIPAA minimum necessary standard, HIPAA-covered entities are required to make reasonable efforts to ensure that access to [personal health information] is limited to minimum necessary information to accomplish the intended purpose of a particular use, disclosure, or request."[20] The minimum necessary standard serves as a protection against misuse of health information. This standard applies to both covered entities and their business associates, and while there is some discretion

---

[11] Copeland, *supra* note 1.

[12] *Id*.

[13] *Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVICES (April 17, 2020, 2:50 PM), http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[14] *Id*.

[15] *Id*.

[16] Newman, *supra note* 9 at 436.

[17] *Ascension and Google working together on healthcare transformation,* BUSINESSWIRE, (Nov. 11, 2019), https://www.businesswire.com/news/home/20191111005613/en/Ascension-Google-working-healthcare-transformation/.

[18] Big Data's Role in Precision Public Health, PMC U.S. Nat'l Lib. of Med., NAT'L INST. OF HEALTH, (Mar 7, 2018), www.ncbi.nlm.nih.gov/pmc/articles/PMC5859342/.

[19] The HIPAA Minimum Necessary Standard, HIPAA JOURNAL, (Jun 23, 2016), https://www.hipaajournal.com/ahima-hipaa-minimum-necessary-standard-3481/.

[20] *Id*.

in the application of the rule, any decisions should be supported by rational justification that should factor in privacy and security.[21] It is on both Ascension and Google to make their own determination of what information is absolutely necessary to carry out their goals, and to protect all other personal health information.

There is no reasonable justification for why Google would need identified medical records for their machine learning programs. If they require complete medical histories and information, the name and exact birthdate of a patient is not important. Although it is easier and cheaper to just transfer all records without de-identifying, hashing, or assigning random numbers to each patient, it is not a significant barrier when weighed against patient privacy. Names and birthdates are not minimum necessary information for any machine learning algorithm, it will work just as well based on a randomly assigned ID. The trend in all areas of big data is to require the use of de-identified data in these models, and health care records should not be an exception. The Google whistleblower raised important concerns about the unprecedented access that companies like Google are getting to the personal medical records of Americans, and the responsibility that covered entities, like Ascension, have when transferring patient records. The minimum necessary standard should continue to be present in the minds of every covered entity and business associate as they determine what data to protect.

Data is valuable, but so is privacy, and if we are concerned as Californians about companies like Google selling our data without our knowledge when it comes to our shopping preferences, why should we not be more concerned with what they will do with our medical history?

---

[21] *Id*.