Project Nightingale – The Case for Google
By Monica Tapavalu[1]

It is no secret that major tech companies are entering the healthcare space by collaborating with healthcare providers to create new tools for patients, hospitals, and insurers.[2] On November 11, 2019, the Wall Street Journal first reported on the previously unknown Project Nightingale, a partnership between tech giant Google and Ascension, the second largest healthcare provider in America.[3] This partnership focused on the collection and processing of approximately 50 million Ascension patient's health information.[4] Patient data included personally identifiable demographics, lab results, doctor diagnoses, and hospitalization records among other categories.[5] Ascension permitted Google to use this data to create new software that runs on advanced artificial intelligence (AI) to help make suggestions about a patient's diagnosis, prescriptions, and treatment.[6] This internal infrastructure would also serve to make recommendations for enforcement of a hospital's narcotics policy.[7] The Wall Street Journal article reported on concerns from a whistleblower, who later published his/her own article in The Guardian.[8] This individual was particularly concerned with the manner in which the data was being collected and shared.[9] Since the announcement of this partnership, both Google[10] and Ascension[11] have released statements addressing concerns from the whistleblower. Consequently, this partnership has highlighted two major points of contention for the public: (1) is this type of data transfer, absent consent, legal under the Health Insurance Portability and Accountability Act (HIPAA)? And (2) does society want major tech companies such as Google accessing their health information?

Shortly after the Wall Street Journal's reports, the U.S. Department of Health and Human Services Office for Civil Rights announced that it would open a federal inquiry.[12] Google and Ascension have recently been questioned by members of the Senate[13] and the House of Representatives regarding current data privacy concerns.[14] Google has stressed that this partnership "adheres to industry-wide regulations

---

[1] J.D. 2020, Santa Clara University School of Law. This article was published to complete the requirements for the Privacy Law Certificate at Santa Clara University School of Law in conjunction with the article written by Elizabeth Magnan.

[2] Nancy Huynh, *How the "Big 4" Tech Companies Are Leading Healthcare Innovation,* HEALTHCARE WEEKLY (Feb. 27, 2019), https://healthcareweekly.com/how-the-big-4-tech-companies-are-leading-healthcare-innovation/.

[3] 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.

[4] Rob Copeland & Sarah E. Needleman, *Google's 'Project Nightingale' Triggers Federal Inquiry,* THE WALL STREET JOURNAL (Nov. 12, 2019), https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867.

[5] Copeland, *supra* note 2.

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

[7] *Id.*

[8] *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.

[9] *Id.*

[10] Shaukat, *supra* note 5.

[11] *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/.

[12] Copeland, *supra* note 3.

[13] Jessica Davis, *Senators Press Ascension on Data Sharing Agreement with Google,* HEALTH IT SECURITY (Mar. 4, 2020), https://healthitsecurity.com/news/senators-press-ascension-on-data-sharing-agreement-with-google.

[14] Jessica Davis, *House Dem Presses Google on Health Data Sharing Activities, Security,* HEALTH IT SECURITY (Dec. 10, 2019), https://healthitsecurity.com/news/house-dem-presses-google-on-health-data-collection-activities.

(including HIPAA) regarding patient data, and comes with strict guidance on data privacy, security and usage."[15] Moreover, Google has highlighted that "[w]e have a Business Associate Agreement (BAA) with Ascension, which governs access to protected health information for the purpose of helping providers support patient care."[16] In fact, similar partnerships and BAA's are not foreign to Google. In their statement, Google points out their many partnerships with healthcare providers and health research entities for the purpose of healthcare technology development, such as McKesson and The National Institute on Aging.[17]

Under HIPAA, healthcare providers are permitted to use patients' health information for its own healthcare operations, which includes "outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities,"[18] as well as "population-based activities relating to improving health or reducing health care costs."[19] The reality is that healthcare providers rely on a vast amount of business associates to perform functions that involve the use or disclosure of protected health information.[20] Business associates are defined in HIPAA as parties that are subcontracted by healthcare providers to provide services and are subject contractual obligations.[21] A BAA must include limiting language that restricts the business associate's use and disclosure of patient information to carry out necessary functions and in a way that resembles the method used if the information was being processed by the healthcare provider itself.[22] These agreements allow healthcare providers to tap into expertise and resources to which they do not otherwise have access. Healthcare providers have the ability to limit the permissible use of the business associate and control their access and disclosure of protected health information.

The concerns that Google's use will be outside of the permitted scope is reasonable, but erroneous. HIPAA prohibits business associates from using a patient's information for their own purposes without explicit patient consent.[23] Fears that Google will be using this data for target marketing have been extinguished as Google's President, Tariq Shaukat, declared in Google's public statement that they will not be using the data for their own marketing purposes.[24] The public's skepticism is understandable; however, it should not prohibit technology companies from accessing patient information to develop AI. Secure healthcare data sharing is vital for developing higher-quality care, early medical intervention , medical training and fraud detection.[25] The more data the AI ingests, the more valuable insights it may potentially uncover.[26] AI, such as that developed by Google, is an important step to improve healthcare operations. The method and scale this technology introduces allows healthcare providers the potential to evaluate outcomes and develop recommendations on clinical practice improvements that would not otherwise be achievable.

Apprehensions over Google's and Ascension's transparency of this partnership are mistaken, but understandable. A recent study showed that this anxiety typically stems from not understanding enough

---

[15] Davis, *supra* note 13.
[16] *Id.*
[17] *Google Cloud for healthcare and life sciences,* GOOGLE CLOUD (Mar. 20, 2020, 10:32 AM), https://cloud.google.com/solutions/healthcare-life-sciences#our-customers.
[18] 45 CFR § 164.501.
[19] *Id.*
[20] *Health Information Privacy,* U.S. DEP'T OF HEALTH & HUMAN SERVICES (Mar. 27, 2020, 1:36 PM), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.
[21] 45 CFR § 164.501.
[22] *Id.*
[23] 45 C.F.R. §164.502(e).
[24] Shaukat, *supra* note 5.
[25] *No longer science fiction, AI and robotics are transforming healthcare,* PRICEWATERHOUSECOOPERS (Apr. 3, 2020, 10.44am), https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html.
[26] Leor Distenfeld, *Data in, insights out: why AI needs robust data to be effective*, MEDIUM (Apr. 12, 2018), https://medium.com/swlh/data-in-insights-out-why-ai-needs-robust-data-to-be-effective-2168b5c1730b.

about AI or how AI works, as well as concerns that the technology might not understand them.[27] Moreover, Americans have little confidence in the accountability of the organizations that hold their data.[28] However, it is common practice for healthcare providers not to notify patients or staff of each third party that is involved in administering operational and treatment functions. There are far too many third parties operating on various levels to explicitly collect consent for data use without additional burden. Furthermore, maintaining a competitive advantage is why companies seek to prevent public disclosure of software developments, [29] it is reasonable to deduce that this would extend to life-changing AI. The incentives for confidentiality are much more advantageous for healthcare providers and patients in the long term.

Much of the backlash was also focused on why the information was not de-identified, and critics are skeptical of how Google will use the identifiable information.[30] Under HIPAA, a healthcare provider may permit business associates to use the patient information to create potentially valuable de-identified information.[31] Although Google and Ascension have not specifically addressed why information was not de-identified, we can suspect that necessary developments require that the information be identifiable. Even before the announcement of this partnership, there had been increasing privacy concerns over Google's access to health data through its acquisition of Fitbit in 2019.[32] Google is one of many (?) big tech companies that are now expanding their reach into the healthcare industry through structured data and AI.[33] Data is valuable and, by permitting the sharing of data, companies with time and resources are able to revolutionize their services and products to make meaningful impact.

Precise data is required to properly train machine learning for accuracy. There is a legitimate reason to train machines on identifiable data, such as for the maintenance of humans, compliance, safety purposes and health planning. Large amounts of data are required for this. Medicine learning requires understanding every patient individually and unique variables. When information is redacted or de-identified we cannot learn about new correlations.[34] Everything needs to be determined on a detailed, specific level. Furthermore, we cannot predict what we need in the future. For every new hypothesis, if we were to revisit redacted clinical data to evaluate why a particular outcome emerged, we will not have access to those variables if they are always de-identified.[35] Especially during this time of medical uncertainty amid the COVID-19 pandemic, having the potential to efficiently identify and prevent diseases, develop treatments and reduce costs of health care can only improve a problematic situation. As unappealing as the reality may be, to develop life saving devices and implement treatment, our best tools require as much information and sources as possible. Countries and entities that fail to recognize this will be left behind.

---

[27] Accenture Consulting, *2018 Consumer Survey on Digital Health, US Results* (2018), available at https://www.accenture.com/t20180306t103559z__w__/us-en/_acnmedia/pdf-71/accenture-health-2018-consumer-survey-digital-health.pdf.

[28] Brooke Auxier, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[29] John W. Mashni, *Trade Secrets: The Big Thing for Tech Companies*, FOSTER SWIFT COLLINS & SMITH PC, ATTORNEYS (May 15, 2014), https://www.michiganitlaw.com/Trade-Secrets-Tech-Companies.

[30] Copeland, *supra* note 3.

[31] 45 C.F.R. §164.506.

[32] Ed Pilkington, *Google's secret cache of medical data includes names and full details of millions – whistleblower,* THE GUARDIAN (Nov. 12, 2019), https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information.

[33] Huynh, *supra* note 1.

[34] *Using Machine Learning with Health Data: The Challenges and Pitfalls,* INSIDE BIG DATA (Jul. 13, 2017), https://insidebigdata.com/2017/07/13/using-machine-learning-health-data-challenges-pitfalls/.

[35] Huynh, *supra* note 1.

Conclusion

The primary purposes of HIPAA are to improve efficiency in the healthcare industry, prevent healthcare fraud, and prohibit discrimination from medical insurance coverage.[36] Regulations aimed at protecting individuals from adverse action are imperative and should be of the utmost importance. However, sharing information does not hinder these purposes, nor does it harm society. The focus should not be on stifling data sharing, but on utilizing the wealth of information available to us to empower key participants to further the advancement of health knowledge and care.

[36] *What is the Purpose of HIPAA?,* HIPAA JOURNAL (Oct. 18, 2017), https://www.hipaajournal.com/purpose-of-hipaa/.