IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

MATT DINERSTEIN, individually and on behalf of all others similarly situated, *Plaintiff*, v. GOOGLE, LLC, a Delaware limited liability company, and THE UNIVERSITY OF CHICAGO MEDICAL CENTER, an Illinois not-for-profit corporation, THE UNIVERSITY OF CHICAGO, an Illinois not-for-profit corporation, *Defendants*.	Case No.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Matt Dinerstein brings this Class Action Complaint and Demand for Jury Trial against Defendants Google, LLC, The University of Chicago Medical Center, and The University of Chicago (collectively referred to as the "University" or "University of Chicago"). Plaintiff, individually and on behalf of all others similarly situated, alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. While tech giants have dominated the news over the last few years for repeatedly violating consumers' privacy, Google managed to fly under the radar as it pulled off what is likely the greatest heist of consumer medical records in history. The compromised personal information is not just run-of-the-mill like credit card numbers, usernames and passwords, or even social security numbers, which nowadays seem to be the subject of daily hacks; rather, the

personal medical information obtained by Google is the most sensitive and intimate information in an individual's life, and its unauthorized disclosure is far more damaging to an individual's privacy.

2. Beginning in 2017, Google set in motion a plan to make its most significant play in the healthcare space. This plan had two key components: (1) obtain the Electronic Health Record ("EHR") of nearly *every patient* from the University of Chicago Medical Center from 2009 to 2016; and (2) file a patent for its own proprietary and commercial EHR system that wouldn't be published until well after it had obtained hundreds of thousands of EHRs from the University.

3. EHRs contain patients' highly sensitive and detailed medical records, including records revealing not only a person's height, weight and vital signs, but whether they suffer from diseases like AIDS, cancer, sickle cell, depression, sarcoidosis, or diabetes, or went through a medical procedure like an abortion, transplant, or mastectomy. In short, EHRs are the most personal and sensitive information that exist about a person.

4. The disclosure of EHRs here is even more egregious because the University promised in its patient admission forms that it would *not* disclose patients' records to third parties, like Google, for commercial purposes. Nevertheless, the University did not notify its patients, let alone obtain their express consent, before turning over their confidential medical records to Google for its own commercial gain.

5. In an attempt to provide the public a false sense of security over the legitimate privacy concerns with these practices, Google and the University claimed the medical records were de-identified. But that's incredibly misleading. The records the University provided Google

included detailed datestamps[1] and copious free-text notes. As shown below, Google—as one of the most prolific data mining companies—is uniquely able to determine the identity of almost every medical record the University released.

6. This ability is only increased by and through Google's direct subsidiary, DeepMind, an international leader in artificial intelligence machine learning. In the year following Google's massive medical data grab, it fully absorbed and took control of a division of DeepMind known as "DeepMind Health," for the specific purpose of analyzing medical records and creating commercial products. Google's access to DeepMind's technology allows it to find connections between various data points (*i.e.* from EHRs and Google users' data).

7. Google spent the last decade attempting to gain a foothold in the trillion-dollar per year healthcare industry. But, to develop the type of healthcare technologies most in line with its data analytics and mining platforms, Google needed access to massive amounts of identifiable medical records. To a company like Google—best known for its ubiquitous search engine, but in reality, one of the largest data mining companies in the world—access to that type of data is extremely elusive.

8. To be sure, Google's overtures for such detailed and identifiable records from hospitals, researchers, and healthcare providers alike were all uniformly rebuffed. That is, of course, until Google came across The University of Chicago.

9. The University provided Google a partner willing to turn over the information that it desperately needed. Indeed, the University—seeking not much more than notoriety for its collaboration with Google in the development of healthcare products—was happy to turn over the confidential, highly sensitive and HIPAA-protected records of every patient who walked

[1] The term "datestamp," in the medical field, is inclusive of both date and time.

through its doors between 2009 and 2016. Ultimately, by getting the University to turn over these records, Google quietly pulled off a feat that other tech giants (like Facebook) have had to abandon under mounting public pressure for other gross privacy violations.[2]

10. And as if all of this weren't bad enough, the University also engaged in a cover up to keep the breach out of the public eye so as to avoid the public backlash. The cover up is particularly egregious because the University had a legal duty to inform its patients and the authorities of the unauthorized transfer of their medical records to Google. While this type of public misinformation campaign may be expected from a tech company that has been known to play fast and loose with the information of its customers, the fact that a prominent institution like The University of Chicago would act in such a way is truly stunning.

11. Accordingly, this Complaint seeks all appropriate damages and injunctive relief to address, remedy, and prevent further harm to Plaintiff and the Class resulting from Defendants' gross misconduct.

PARTIES

12. Plaintiff Matt Dinerstein is a natural person and a citizen of the State of Illinois.

13. Defendant Google, LLC, is a limited liability company existing under the laws of the State of Delaware, with its principal place of business located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

14. Defendant The University of Chicago Medical Center is a not-for-profit corporation existing under the laws of the State of Illinois, with its principal place of business located at 5841 South Maryland Avenue, Chicago, Illinois 60637.

---

[2] *Facebook sent a doctor on a secret mission to ask hospitals to share patient data*, CNBC, https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html?cid=sm_npd_nn_tw_ma (last visited on June 26, 2019).

15. Defendant The University of Chicago is a not-for-profit corporation existing under the laws of the State of Illinois, with its principal place of business located at 5801 South Ellis Avenue, Chicago, Illinois 60637.[3]

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii) the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iii) none of the exceptions under that section apply.

17. This Court has personal jurisdiction over Defendants because they conduct business in this District and the wrongful conduct giving rise to this case occurred in, was directed to, or emanated from this District. This Court further has personal jurisdiction over Defendants The University of Chicago Medical Center and The University of Chicago because they are headquartered in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants The University of Chicago Medical Center and The University of Chicago maintain their headquarters and principal place of business in this District, and a substantial part of the events giving rise to Plaintiff's Complaint occurred in this District.

FACTUAL BACKGROUND

I. Detailed and Identifiable Medical Records are the Most Valuable Consumer Data, and the Hardest to Obtain.

19. With the rise of the data mining industry, corporations have started gathering

[3] The University of Chicago Medical Center and The University of Chicago are fully integrated entities that have acted jointly in this case. The University of Chicago Medical Center and The University of Chicago are jointly managed and share employees.

untold amounts of data regarding consumers' daily lives, including what they do on their phones, and computers, where they travel each day, and even what they purchase in retail stores. From this, data miners and brokers can build detailed portfolios about consumers that are then bought and sold for a variety of purposes.

20. A key component of any data portfolio is the status of a consumer's health. While data points such as purchase histories, search engine and browsing histories, as well as social media posts can provide insight into certain health problems, a clear picture of a consumer's health remains largely a black hole for data miners. The only substantial remedy to this problem is access to detailed and complete medical records.

21. A multi-billion-dollar industry has arisen in response to this need.[4] Pharmacies, insurance companies, and other medical organizations—including federal and many state health departments—provide limited medical information to data brokers. Three quarters of all retail pharmacies send some portion of their electronic records to these companies. While this data is largely de-identified, data brokers are able to make numerous assumptions about the data in order to make it into a marketable product.[5]

22. These data points are often incomplete in other ways beyond de-identification. In most instances, the data points are merely a snapshot of a small part of a consumer's overall health (*e.g.*, a specific prescription or a single ailment, etc.). This type of data will rarely, if ever, show a complete medical history or in-depth accounting of medical ailments and procedures over

---

[4] *How Data Brokers Make Money Off Your Medical Records*, SCIENTIFIC AMERICAN, https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records (last visited on June 26, 2019).

[5] *Your private medical data is for sale – and it's driving a business worth billions*, THE GUARDIAN, https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns (last visited on June 26, 2019).

time.[6] That data, largely contained only in the records of doctors and hospitals, is far more rare and is viewed as a "Holy Grail" of health information for any data miner.[7]

23. A complete health record is an extremely sensitive data set that provides insight into the most personal aspects of an individual's life. It can shed light on chronic conditions, life-threatening illnesses, whether a person has addiction issues, disabilities, and issues related to pregnancy, along with personal details such as sexual preferences, gender nonconformity, and sexually transmitted diseases.

24. The details of an individual's medical history are of significant value to a variety of interested parties, including employers, schools, governments, insurance companies, lenders, retail marketers, and obviously, companies in the health care business. These entities can rely on consumers' records to make decisions about whether to lend money, how to price insurance products, whether to hire a person, and even identify reasons to discriminate.

25. Full medical records are so sensitive, and so sought after, that Congress created a comprehensive statutory regime, known as the Health Insurance Portability and Accountability Act ("HIPAA"), to prevent their unauthorized disclosure. HIPAA established rules that require healthcare organizations to limit who can access, view, or share health data. It is meant to ensure that any information disclosed to healthcare providers (*e.g.*, doctors and hospitals) and health plans (*e.g.*, insurance companies), or information that is created by them, is subject to strict

---

[6] *The incredible potential and dangers of data mining health records*, THE WASHINGTON POST, https://www.washingtonpost.com/news/innovations/wp/2014/10/01/the-incredible-potential-and-dangers-of-data-mining-health-records/?utm_term=.f92ac1b63800 (last visited on June 26, 2019).

[7] *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME, http://time.com/4588104/medical-data-industry (last visited on June 26, 19); *see also The Hidden Global Trade in Patient Medical Data*, YALEGLOBAL ONLINE, https://yaleglobal.yale.edu/content/hidden-global-trade-patient-medical-data (last visited on June 26, 2019).

security controls. Patients are also given control over who their information is released to and who it is shared with.

26. Besides the obvious obligations that health-care providers, like the University, have to act in the best interest of their patients' health, a primary duty of any health care provider during and long after patients are cared-for—regardless of whether in connection with a run-of-the-mill visit to the doctor's office or life-saving trip to the emergency room—is to protect their privacy and secure their medical records in accordance with HIPAA.

27. Without HIPAA, data miners like Google, in conjunction with hospitals like the University, could create a thriving marketplace for medical data. Companies would willingly pay millions of dollars for complete medical records, which they would analyze, repackage and sell to thousands of clients.

28. Fortunately, HIPAA does exist. The only question that remains is whether entities like Defendants choose to follow it.

II. An Overview of HIPAA.

29. HIPAA was enacted and became effective in 1996. Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. However, the increased reliance on electronic information systems for storing medical information and facilitating treatment created a rising need for regulation.

30. HIPAA required the federal government to develop regulations protecting the privacy and security of certain health information. In response, the government published the HIPAA Privacy Rule and the HIPAA Security Rule.

31. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health

Information, establishes national standards for the protection of certain health information. The Security Rule establishes a national set of security rules for protecting certain health information that is held or transferred in electronic form.

32. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities"[8] must put in place to secure individuals' "electronic protected health information."[9]

33. Violations of HIPAA carry significant fines and penalties of up to $50,000 per violation. Additionally, covered entities and specified individuals who "knowingly" obtain or disclose individually identifiable health information can face imprisonment of up to one year.

34. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services create rules to streamline the standards for handling individually identifiable personal health information. The Department of Health and Human Services established standards to protect such electronic personal health information from unauthorized disclosure. These standards require entities, such as the University, to adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of personal health records.

35. When personal health information is de-identified (*i.e.*, a process whereby identifiers are removed from the health information), HIPAA does not restrict the use or

---

[8] "Covered entities" include health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA. *See* Summary of the HIPAA Security Rule, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited on June 26, 2019).

[9] *Id*.

disclosure of such information. Under HIPAA, health information that does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual, is not considered individually identifiable health information.

36. Here, because Defendants touted to the public that the mass transfer of the University's medical records were de-identified, HIPAA's de-identification provisions apply.

37. There are two methods to achieve de-identification of protected health information.

38. The first, referred to as the "Expert Determination" method, requires:

> (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
>
> (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
>
> (ii) Documents the methods and results of the analysis that justify such determination;

The second method for de-identification is referred to as the "Safe Harbor." According to this method, the following categories of information must be removed from personal health records to be properly de-identified:

> (A) Names; (B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census…; (C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (E) Fax numbers; (M) Device identifiers and serial numbers; (F) Email addresses; (N) Web Universal Resource Locators (URLs); (G) Social

> security numbers; (O) Internet Protocol (IP) addresses; (H) Medical record numbers; (P) Biometric identifiers, including finger and voice prints; (I) Health plan beneficiary numbers; (Q) Full-face photographs and any comparable images; (J) Account numbers; (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section "Re-identification"]; and (K) Certificate/license numbers.

39. As described below, the Defendants did not follow either of these rules in disclosing and accepting hundreds of thousands of medical records.

III. The University of Chicago is Obligated to Protect the Medical Records of Millions of Patients.

40. The University holds itself out as following the highest standards of patient care and being among the highest rated and most awarded hospitals in the world,[10] claims which extend to their commitment to patient privacy and the protection of medical data. The University widely represents that it follows HIPAA and other applicable laws, takes patient privacy seriously, and describes how it will protect patient medical records.

41. The records governed by HIPAA are exactly the type of medical records in the possession of the University. Each time a patient is seen, whether for a brief outpatient procedure or a month-long in-patient stay, the University collects detailed information about their current and past health conditions, as well as creates sensitive new data while the individual is treated. Individuals entrust their most personal information, experiences, and physical and mental hardships to the medical staff of the University. This can include genetic information, family health histories, details of sexual encounters, mental illness or a terminal diagnosis. In return, patients expect that the University will act accordingly and protect their privacy.

42. Over decades of operation, the University has collected and stored billions of data

[10] Award and Distinctions, *UChicago Medicine*, http://www.uchospitals.edu/about/awards/ (last visited on June 26, 2019).

points through millions of patient medical records.

43. From both a legal and ethical standpoint, it is unquestionable that the University is obligated to protect patient data, prevent its unauthorized disclosure, and act in the best interests of its patients. It is equally obvious that the University's patients do not want, and do not consent to, the transfer of their medical records to a third-party data miner intent on using them for commercial purposes.

44. The obligation to protect patient data at the University is heightened by the socio-economic makeup of its patients. A significant portion of the patients treated at the University are socially and economically disenfranchised, making them far less able to vindicate and advocate for their privacy rights.

IV. An Overview of Google and its Aggressive Efforts to Enter the Trillion-Dollar Per Year Healthcare Industry.

45. Although primarily recognized for its search engine, Defendant Google operates one of the most far reaching and comprehensive data mining machines in the world. The Wall Street Journal recently noted that,

> Google Analytics is far and away the web's most dominant analytics platform. Used on the sites of about half of the biggest companies in the U.S., it has a total reach of 30 million to 50 million sites. Google Analytics tracks you whether or not you are logged in. Meanwhile, the billion-plus people who have Google accounts are tracked in even more ways. In 2016, Google changed its terms of service, allowing it to merge its massive trove of tracking and advertising data with the personally identifiable information from our Google accounts…. Google also is the biggest enabler of data harvesting, through the world's two billion active Android mobile devices.[11]

46. With *billions* of monthly active users, Google has access to an exorbitant amount

[11] *Who Has More of Your Personal Data Than Facebook? Try Google*, THE WALL STREET JOURNAL, https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401 (last visited on June 26, 2019).

of personal consumer data, including Internet web browsing histories (Google Chrome), Internet searches (Google Search), physical locations (Google Maps and Waze), personal and work email (Gmail), and mobile devices (Android). This wealth of information feeds into Google's highly profitable analytics and advertising platform, which makes up virtually all of its $110.8 billion of annual revenues.

47. While analytics and advertising are its primary source of income, Google constantly looks to develop new products and services, and enter new markets. One market it has been aggressively trying to enter is the trillion-dollar per year healthcare industry.

a. Google Research

48. Over the last decade, Google has invested heavily in health-related products and services, including:

- Introducing G Suite (*i.e.*, Gmail, Docs, Drive, Calendar, and other cloud services) for healthcare businesses;
- Developing Google Cloud (*i.e.*, Google's cloud storage and computing platform) for HIPAA compliant workloads;
- Creating Google Genomics, which is Google's cloud platform that analyzes and stores massive amounts of human genetic data (*i.e.*, DNA);
- Launching Google Fit, which is a service that monitors individual's physical activity, steps, and caloric intake;
- Adding "symptom search" and "health cards" to Google Search, which allows consumers to more easily research answers to common health-related questions;[12] and
- Making "big bets in healthcare and life sciences" including spending hundreds of millions investing in and acquiring healthcare companies like Calico, DeepMind, and Verily.

[12] In fact, 1 in 20 Google searches are for health-related information. *See* Prem Ramaswami, *A remedy for your health-related questions: health info in the Knowledge Graph*, GOOGLE (Feb. 10, 2015), https://googleblog.blogspot.com/2015/02/health-info-knowledge-graph.html (last visited on June 26, 2019).

49. Google also created what it calls its Google Research healthcare team. Google Research is Google's in-house research center that it markets as an academic-type think tank or research center (in reality, it's just a product research and development division). The healthcare team, in turn, researches opportunities for applying Google technologies—machine learning and artificial intelligence ("AI"), in particular—to healthcare. According to its marketing materials, Google's healthcare team believes:

> "AI is poised to transform medicine, delivering new, assistive technologies that will empower doctors to better serve their patients. Machine learning has dozens of possible application areas, but healthcare stands out as a remarkable opportunity. . . ."[13]

50. Google was especially interested in using its machine learning models to predict healthcare events, like detecting a patient's heart attack hours or even days in advance.

51. But Google had difficulty gaining a foothold in the predictive health analytics industry. Indeed, Google's major hurdle to predicting healthcare events, as described above, was a lack of access to massive amounts of personal health data, which consumers are not eager to share with data miners and thus, healthcare providers are prohibited from doing so. Google knew this, so it attempted a work-around.

52. In 2008, Google attempted to gather consumer medical data by developing a service that let consumers organize and store their personal health data and medical records on Google's platform. The service barely got off the ground, however. After a short period of time, it was discontinued for a lack of consumer participation.

53. Thereafter, Google went looking for new avenues of access to patient data.

---

[13] *Healthcare*, GOOGLE RESEARCH, https://research.google.com/teams/brain/healthcare/ (last visited on June 26, 2019).

b. DeepMind

54. In 2014, for $520 million, Google acquired a tiny startup named DeepMind that focused on bringing artificial intelligence and advanced machine learning to, among others, the healthcare industry.

55. Following this acquisition, Google, in part through DeepMind, embarked on a campaign, veiled as well-intentioned research, to obtain millions of medical records from health care organizations.

56. Initially, Google and DeepMind participated in a 2015 "study" that processed patient data from the Royal Free NHS Foundation Trust. The medical record sharing there raised serious concerns about privacy and patient consent. The Information Commissioner's Office, a UK data protection watchdog, stated, "[o]ur investigation found a number of shortcomings in the way patient records were shared for this trial . . . Patients would not have reasonably expected their information to have been used in this way, and the Trust could and should have been far more transparent with patients as to what was happening." It concluded that the agreement with Royal Free "failed to comply with data protection law."[14]

57. DeepMind, in response, stated "in our determination to achieve quick impact when this work started in 2015, we underestimated the complexity of the NHS and of the rules around patient data, as well as the potential fears about a well-known tech company working in

[14] *See Royal Free breached UK data law in 1.6m patient deal with Google's DeepMind,* THE GUARDIAN, https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act (last visited on June 26, 2019); *see also The Information Commissioner, the Royal Free, and what we've learned*, https://deepmind.com/blog/ico-royal-free (last visited on June 26, 2019).

health."[15]

58. While their statements were meant to be an apology and included promises to protect patient privacy, it did not change Google's course.[16]

59. During this time, Google and DeepMind widely propagated the narrative that DeepMind would continue to operate independently and outside the reach of Google, and that Google would not have direct access to patient records.

c. Google's Commercialization Plans

60. However, shortly after Google acquired hundreds of thousands of records from the University of Chicago, that narrative finally fell apart. In November 2018, Google announced that it would fully absorb and take control of DeepMind Health, separating it from DeepMind itself.[17] As such, any supposed wall protecting health data collected and processed by DeepMind was gone. And furthermore, Google now has at its disposal all the advanced capabilities possessed by DeepMind to apply to the health records acquired from the University of Chicago.[18]

---

[15] *The Information Commissioner, the Royal Free, and what we've learned*, DeepMind.com, https://deepmind.com/blog/ico-royal-free/ (last visited on June 26, 2019).

[16] Google has since gained access to 700,000 medical records through the US Department of Veterans Affairs. It remains unclear, what, if any, consent veterans provided to share their medical records with Google or the level of detail included in those records. *Researching patient deterioration with the US Department of Veterans Affairs*, DeepMind.com, https://deepmind.com/blog/research-department-veterans-affairs/ (last visited on June 26, 2019).

[17] *DeepMind Is Handing DeepMind Health Over To Google*, FORBES, https://www.forbes.com/sites/samshead/2018/11/13/deepmind-is-handing-over-deepmind-health-to-google/#6db706b72d55 (last visited on June 26, 2019); *Why Google Just Tightened Its Grip On DeepMind*, Forbes, https://www.forbes.com/sites/parmyolson/2018/11/14/why-google-just-tightened-its-grip-on-deepmind/#1aa439552789 (last visited on June 26, 2019).

[18] *Google has a responsibility to protect DeepMind data*, Financial Times, https://www.ft.com/content/83e1e46c-ebf0-11e8-8180-9cf212677a57 (last visited on June 26, 2019); *Google, DeepMind and my confidential health records*, Financial Times,

61. Additionally, it is clear that the takeover of DeepMind Health was meant to be a major step toward the full-scale commercialization of Google's health products. As noted by the Financial Times:

> David Feinberg, the former head of the US private healthcare group Geisinger, will run Google Health, *drawing together and commercializing the company's disparate experiments* in everything from diagnosing cancer to managing chronic illness and equipping doctors with more technology… '[Feinberg's] expertise is on the operational side of the health payer-provider space, rather than research. His role will be to figure out a go-to-market strategy, how to deploy and sell tools to hospitals, health insurance carriers and patients,' said Nikhil Krishnan, health analyst at CBInsights, who has authored an in-depth report on Google's healthcare business.[19] (Emphasis added).

62. Predictably, Google's efforts culminated in a recently revealed patent application for its own electronic health records system, which "include a computer memory storing aggregated EHR data from millions of patients; a computer executing deep learning on those records in a standardized data structure format, and an interface for clinicians displaying salient facts from the patient's past and predicted future clinical events."[20] Google submitted this application in 2017, demonstrating its clear intent to commercialize the University's medical records prior to obtaining them. Specifically, as noted below, the application discusses providing its EHR product in a "fee for service, subscription, standalone product, or other business model."

---

https://www.ft.com/content/2ee8c190-ed28-11e8-8180-9cf212677a57 (last visited on June 26, 2019).

[19] *Inside DeepMind as the lines with Google blur*, Financial Times, https://www.ft.com/content/c26893d0-e9b0-11e8-a34c-663b3f553b35 (last visited on June 26, 2019).

[20] *Google Has Its Own EHR Plan*, Politico, https://www.politico.com/newsletters/morning-ehealth/2019/02/04/data-mongers-have-your-number-for-opioid-abuse-501593; *see also* http://pdfaiw.uspto.gov/.aiw?PageNum=0&docid=20190034591 (last visited on June 26, 2019).

> **[0200]** The precise physical location and implementation of the predictive models and related computer or computer system **26** may vary. In some instances it may be physically located at a medical system or hospital serving affiliated facilities, primary care physician offices, and related clinics etc. In other situations it may be centrally located and receive EHRs and transmit predicted future clinical events and related prior medical events over wide area computer networks and service a multitude of unrelated healthcare institutions in a fee for service, subscription, standalone product, or other business model. In all situations appropriate data security and HIPPA compliance procedures are in place.

d. Google is Not Alone in its Pursuit of Medical Records; It is Just the Most Successful.

63. Moreover, Google's goal of obtaining these valuable and sensitive records is not unique; rather it is shared by Google's competitors in the data mining space, and as recently revealed, that includes Facebook. By its own description, Facebook had a plan to:

> combine what a health system knows about its patients (such as: person has heart disease, is age 50, takes 2 medications and made 3 trips to the hospital this year) with what Facebook knows (such as: user is age 50, married with 3 kids, English isn't a primary language, actively engages with the community by sending a lot of messages). The project would then figure out if this combined information could improve patient care, initially with a focus on cardiovascular health…. To address these privacy laws and concerns, Facebook proposed to obscure personally identifiable information, such as names, in the data being shared by both sides. However, the company proposed using a common cryptographic technique called hashing to match individuals who were in both data sets. That way, both parties would be able to tell when a specific set of Facebook data matched up with a specific set of patient data. The issue of patient consent did not come up in the early discussions.[21]

64. Yet, Facebook, then under fire for failing to prevent the capture and misuse of at

---

[21] *Facebook sent a doctor on a secret mission to ask hospitals to share patient data*, CNBC, https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html?cid=sm_npd_nn_tw_ma (last visited on June 26, 2019).

least 87 million users' data (along with myriad other privacy scandals), stated "we decided that we should pause these discussions so we can focus on other important work, including doing a better job of protecting people's data and being clearer with them about how that data is used in our products and services."[22]

65. Google, on the other hand, was not yet facing an international privacy scandal, and found a willing partner in the University whose primary focus was apparently not on patient privacy, but rather creating headlines such as "*Google works with University of Chicago to predict medical events*," "*U. of C. Medicine, Google hope to use patterns in patient records to predict health*," and "*UChicago Medicine and Google—a data-driven duo to watch*." While these headlines circulated in the medical industry for a few days, the ramifications of the University's and Google's actions will last far longer.

VI. The University of Chicago Unlawfully Transferred Hundreds of Thousands of Patients' Records to Google.

66. In May 2017, Google announced that it was partnering with The University of Chicago to "research ways to use machine learning to predict medical events." And only months later, the University transferred its EHR to Google, consisting of hundreds of thousands of its patients' medical records.

a. The University did not obtain patients' express consent to disclose their medical records to Google.

67. Prior to transferring these records, the University did not obtain the express consent of its patients to share them for the purposes Google intended to use them for, nor did it

[22] *Facebook is pausing its work on sharing data with hospitals in the wake of the Cambridge Analytica scandal*, BUSINESS INSIDER, http://www.businessinsider.com/facebook-pauses-health-collaboration-after-cambridge-analytica-scandal-2018-4?r=UK&IR=T (last visited on June 26, 2019).

inform them of the incredibly inadequate redactions that would be applied.

68. Through its Notice of Privacy Practices and Admission and Outpatient Agreement and Authorization, the University represented to patients that it would, *inter alia*: protect their medical information, maintain the privacy of their medical information, follow the terms of the Notice of Privacy Practices in keeping their medical information confidential, comply with HIPAA privacy regulations, and comply with any other federal and state laws, including all laws that govern patient confidentiality.

69. The University's Notice of Privacy Practices states that "protecting the privacy of your health information is important" and explicitly warrants that it "will obtain your written permission […] for the sale of your medical information." Nowhere does the University disclose that it would transfer patients' medical records to Google.

70. Likewise, the University's Admission and Outpatient Agreement and Authorization form does not give the University permission to disclose patient's medical records to Google for any purpose whatsoever.

b. The medical records provided to Google by the University contain datestamps that allow Google to identify patients.

71. The University, in conjunction with Google, published an article in a scientific journal describing the results of its research and the methodology it employed in analyzing patients' medical records.[23] The publication revealed that while the EHRs were "de-identified," the datestamps from the University patients' records were maintained. Further, the University's patient's health data "additionally contained de-identified free-text medical notes."

[23] Alvin Rajkomar et al., *Scalable and accurate deep learning for electronic health records,* 1 NPJ DIGITAL MEDICINE, January 2018 at 4, available at https://www.nature.com/articles/s41746-018-0029-1 (last visited on June 26, 2019)

72. The medical records given to Google also contained the following information on both inpatients and outpatients:

a. Patient demographics;
b. Provider orders;
c. Diagnoses;
d. Procedures;
e. Medications;
f. Laboratory values;
g. Vital signs; and
h. Flowsheet data.[24]

73. Only months after the transfer was complete did it become public that the datestamps, along with free-text notes data, were *only provided by the University*, and not by any other hospital working with Google.[25] That's not simply a coincidence or a failure to persuade on the part of Google. Rather, the reason no other hospital, including the other health care providers partnering with Google, provided this type of information is because it would be a *prima facie* violation of HIPAA to share or even receive medical records in this form.

74. Publicly, Google and the University touted the security measures used to transfer and store these records, along with the fact that they had been "de-identified." In reality, these records were not sufficiently anonymized and put the patients' privacy at grave risk.

75. The inclusion of, at the very least, the datestamp data immediately places the transfer of this medical data outside of the Safe Harbor provisions of HIPAA.

76. On information and belief, as required by HIPAA, the University did not perform an expert determination before transferring the medical records to Google; or, alternatively, if it did make that attempt, any finding that "the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient

24 *Id.*
25 *Id.*

to identify an individual who is a subject of the information" was woefully misplaced, as described in the following section.

c. Google's Ability to Re-Identify Medical Records.

77. While Defendants claim to have de-identified the hundreds of thousands of medical records transferred to Google without patient permission, Google is uniquely able to re-identify those records.

i. The Risk of Medical Record Re-Identification is Already a Major Threat.

78. Setting aside Google's specific abilities, the risk of medical record re-identification is high. Researchers with limited access to public data sets and supposedly de-identified medical records have been able to re-identify patients at a shockingly high rate. For example, in one study, researchers at Harvard's Data Privacy Lab were able to re-identify 43% of de-identified medical discharge records utilizing only publicly available data they purchased for $50.[26]

79. In another example, physical activity data was recently used to re-identify thousands of medical records (95% of the available data set) by utilizing artificial intelligence and machine learning. Researchers analyzed the output of fitness trackers and demographic characteristics such as age, gender, education level, annual household income, race, and country of birth.[27] As noted by Anil Aswani of the University of California, Berkeley, one of the study's

---

[26] Latanya Sweeney, *Matching Known Patients to Health Records in Washington State Data*, HARVARD UNIVERSITY, *available at* https://dataprivacylab.org/projects/wa/1089-1.pdf; *see also How Someone Can Re-Identify Your Medical Records*, BLOOMBERG, https://www.bloomberg.com/graphics/infographics/reidentifying-anonymous-medical-records.html (last visited June 26, 2019).

[27] Linda Carroll, *Anonymous patient data may not be as private as previously thought,* REUTERS, https://news.yahoo.com/anonymous-patient-data-may-not-private-previously-thought-190248280.html (last visited June 26, 2019).

authors, "[t]he study shows that machine learning can successfully re-identify the de-identified physical activity data of a large percentage of individuals, and this indicates that our current practices for de-identifying physical activity data are insufficient for privacy … More broadly it suggests that other types of health data that have been thought to be non-identifying could potentially be matched to individuals by using machine learning and other artificial intelligence technologies."[28]

80. Accordingly, sharing medical records, with anyone, that include the identifying information noted above (including datestamps and free-text notes) already has a high probability of being re-identified.

81. However, when the transfer of medical records is made to Google, the ability to re-identify those records becomes a certainty.

ii. Google has Access to Nearly Unlimited Information Capable of Re-Identifying Medical Records.

82. Google is one of the largest and most comprehensive data mining companies in the world, drawing data from thousands of sources and compiling information about individuals' personal traits (gender, age, sexuality, race), personal habits, purchases, and associations.

83. Not unlike recent revelations about Facebook and Cambridge Analytica, Google also creates detailed profiles of millions of Americans for the purpose of predicting how they will react to certain events, what and when they will buy a product, and other behavioral patterns.

84. Based on these detailed profiles alone, Google has access to public and non-public information that could easily lead to the re-identification of the medical records it received

---

28 *Id*.

from the University. And, of course, artificial intelligence and machine learning are the core focus and product of DeepMind Health, Google's newest addition to its healthcare operations and product development.

85. As noted by Bloomberg, "[f]ew companies are better poised to analyze this organism than Google. The company and its Alphabet cousin, Verily, are developing devices to track far more biological signals. Even if consumers don't take up wearable health trackers *en masse*, Google has plenty of other data wells to tap. It knows the weather and traffic. Google's Android phones track things like how people walk, valuable information for measuring mental decline and some other ailments. All that could be thrown into the medical algorithmic soup."[29]

86. Beyond the vast amount of personal information Google possesses, and its incredibly powerful analytics capabilities (including DeepMind Health), Google has in its possession detailed geolocation information that it can use to pinpoint and match exactly when certain people entered and exited the University's hospital.

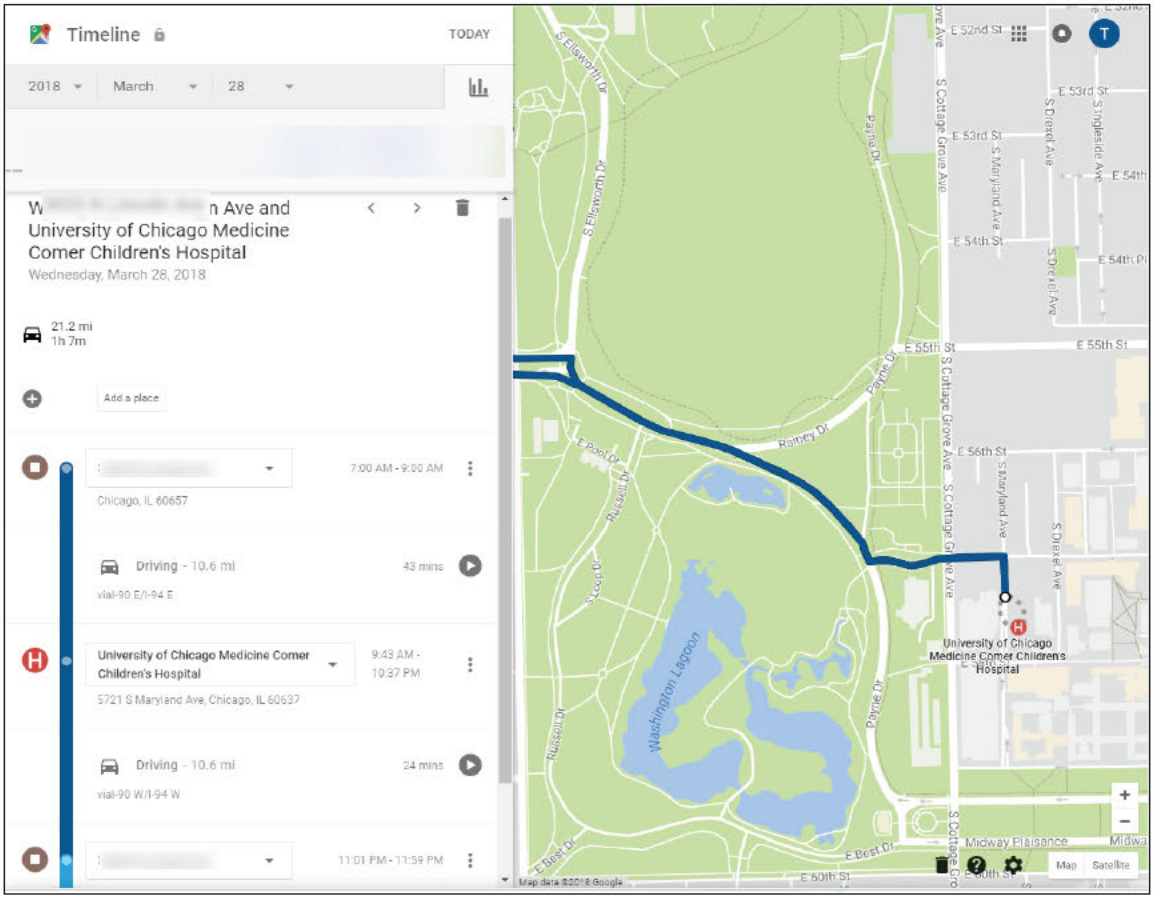
iii. Google Possesses Extremely Precise Geolocation Information on Millions of Consumers.

87. Google tracks consumer locations through a variety of means including users of Android phones and its mobile applications, like Maps and Waze. Likewise, when a consumer uses other Google products, such as its search engine, Google records his or her Internet Protocol address, which corresponds to a very specific physical location. Google is, therefore, able to identify hundreds of millions of individuals' exact location within a matter of feet, if not inches, twenty-four hours a day.

---

[29] *Google Is Training Machines to Predict When a Patient Will Die*, Bloomberg https://www.bloomberg.com/news/articles/2018-06-18/google-is-training-machines-to-predict-when-a-patient-will-die (last visited June 26, 2019).

88. In fact, Google offers a service, called "Timeline," that allows consumers to see the detailed location data that Google possesses. Figure 1 below shows an example screenshot of Timeline, which reveals the (1) individual's exact geographic coordinates; (2) common names and addresses associated with those locations; (3) exact dates and times individuals arrived and departed from specific locations; and (4) the routes traveled between locations (including to and from an individual's home).

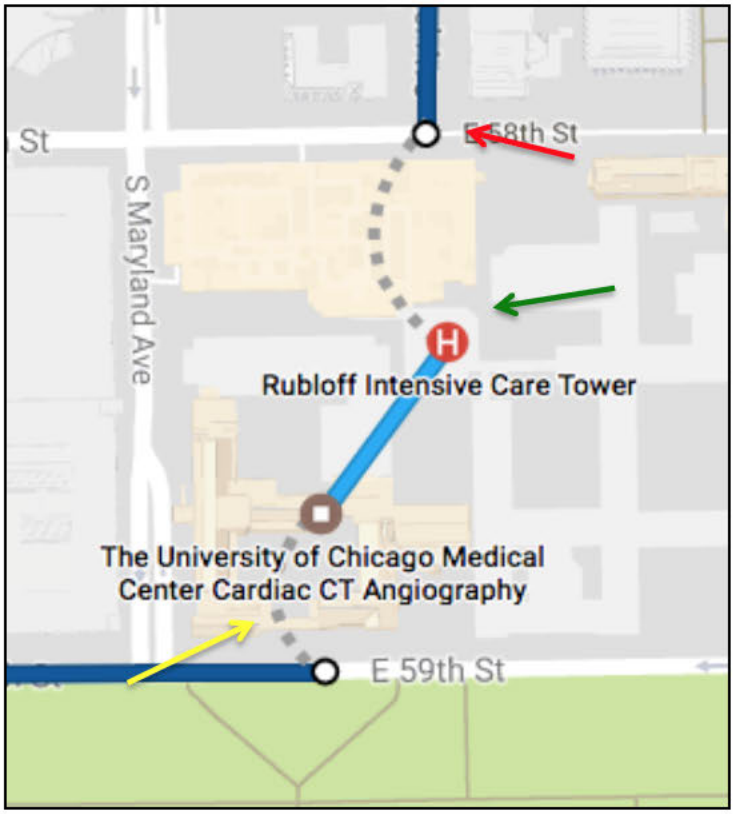


(**Figure 1.**)

89. Consequently, any individual who stepped foot inside The University of Chicago Medical Center, and was one of the billions of users of Google's services, could be identifiable (1) by name; (2) physical and email addresses; (3) having entered the hospital; (4) the exact time

he or she entered; (5) how long he or she stayed inside the hospital; and (6) the exact time he or she left. Likewise, if that person was a repeat patient, the location records would capture the exact same information each time, further narrowing down the patient's identity.[30]

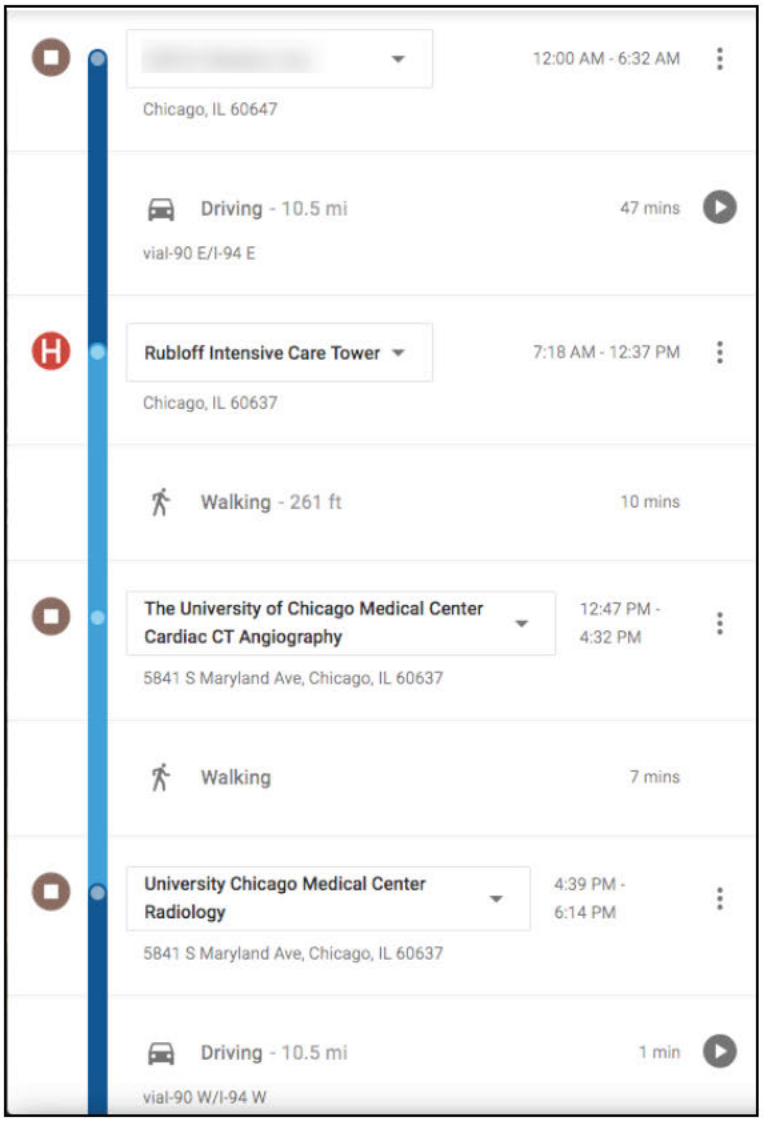
90. Worse still, Google can even identify individuals visiting *specific buildings or departments at the University's Medical Center at specific times*. For example, as shown in Figures 2 and 3, Google can identify an individual traveling to The University Medical Center, walking into the building (highlighted in red), traveling to the intensive care unit (highlighted in green), and leaving the building (specifically by walking, highlighted in yellow).



(**Figure 2.**)

[30] Google not only knows information about the patient, but also that person's spouse, relatives, children, and other associations, and can use that information to further pinpoint a person's exact location (relative to another person) at any given time.

91. Figure 3 shows the corresponding times that the individual was at each specific location or department at The University Medical Center, and traveling to and from.



(**Figure 3.**)

92. Google's access to exact location data is further increased by its vast catalog of WiFi networks around the country. Android phones, in addition to certain Google apps on other platforms, regularly scan and identify nearby WiFi networks (whether a person connects to it or

not) as a way to improve geolocation mapping.[31] The University offers a comprehensive WiFi network at all public buildings on its medical campus,[32] that when a patient connects to it, or even simply in the buildings where the network is live, would identify the location of the network to Google through its prior knowledge of the exact location of that specific WiFi network.

93. This geolocation information, when combined with the exact datestamps for admission and discharge (along with other health events at the hospital) included in the University's medical records, and cross referencing the age, gender, and demographic information with its own data, creates a perfect formulation of data points for Google to identify who the patients in those records really are.[33]

94. If that weren't enough, the University's release of medical records further imperiled patient privacy by including free-text notes. These notes are normally not included in de-identified medical records and themselves create an enormous wealth of data re-identifying the patients themselves.

95. On information and belief, the process used to redact the free-text notes, and its specific results, were not properly audited or verified in an independent manner. As such, there is

---

[31] *How Google Uses Wi-Fi Networks to Figure Out Your Exact Location*, Slate, https://slate.com/technology/2018/06/how-google-uses-wi-fi-networks-to-figure-out-your-exact-location.html (last visited on June 26, 2019) ("Google doesn't merely collect IP-address data to estimate a user's location. Instead, Google retains a detailed map of known Wi-Fi networks and access points. By knowing the exact location of these networks, and your proximity to them, its location services can *gauge your location with roughly 30 feet of accuracy*.") (emphasis added).

[32] *Wireless Internet Access*, UChicago Medicine, https://www.uchicagomedicine.org/patients-visitors/visitor-information/wireless-internet-access (last visited on June 26, 2019).

[33] Google could easily also cross reference consumer search histories with the records themselves (*e.g.*, a University medical record reflects a specific procedure on a specific date, which can be cross referenced with users in the same geographic location performing Google searches about that procedure in the same time period).

no available information regarding the rate of personally identifying information that may have evaded redaction and was transferred to Google. The methods and design of this software, and whether or not it could comprehensively review and redact millions of data points, remains a complete mystery to the patients whose records are now in the hands of Google.

96. Both Google and the University violated HIPAA by sharing and receiving medical records that included sufficient information for Google to re-identify the patients. Both were aware at the time of the transfer that the medical records contained information outside of HIPAA's Safe Harbor provisions, that a competent expert determination was not made, and that the thousands of patients had not given proper consent to allow Google to take possession of the records for the purpose of creating a commercial product.

97. Without question, the University exploited its patients. The University took advantage of the fact that a large number of its patients, due to socio-economic barriers, are not in a position to assert their right to privacy and take steps to ensure that their medical records are not disclosed to a third party for a commercial purpose.

FACTS SPECIFIC TO PLAINTIFF DINERSTEIN

98. Plaintiff Matt Dinerstein was admitted to The University Medical Center on June 4, 2015 and checked out on June 7, 2015 and was again admitted on June 25, 2015 and checked out on June 27, 2015.

99. During his stay, the University generated numerous pages of health records that included sensitive information such as Dinerstein's demographic information, his vitals, diagnoses, procedures, and prescriptions.

100. In 2015, including during his stay at the University Medical Center, Dinerstein used a smartphone with Google applications installed that, on information and belief, collected

his geolocation information and transmitted it back to Defendant Google. During that time, Dinerstein also maintained a Google account.

101. On information and belief, the University disclosed Dinerstein's confidential medical information to Defendant Google. The University did not properly de-identify Dinerstein's medical health records and included datestamps associated with his procedures as well as free-text notes from his doctors and nurses.

102. Dinerstein never gave his written consent—or any consent whatsoever—to the University to disclose his confidential medical information to Google. Similarly, he did not give Defendant Google permission to use his medical records for any purpose, let alone for a commercial purpose.

103. Dinerstein paid health insurance premiums and other fees associated with his treatment at the University.

CLASS ALLEGATIONS

104. **Class Definition:** Plaintiff Matt Dinerstein brings this action on behalf of himself and a class of similarly situated individuals defined as follows:

> All individuals in the United States whose Electronic Health Records were transferred to Google (or any of its related entities) by The University of Chicago (or any of its related entities).

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and the members of their family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel

and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

105. **Numerosity**: The exact number of members of the Class is unknown, but individual joinder in this case is impracticable. The Class likely consists of hundreds of thousands of individuals. Members of the Class can be easily identified through Defendants' records.

106. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:

a. Whether the University's conduct violated the ICFA;

b. Whether the University's conduct constitutes a breach of express contract;

c. Whether the University's conduct constitutes a breach of implied contract;

d. Whether Google's conduct constitutes tortious interference with contract;

e. Whether the Defendants' conduct constitutes intrusion upon seclusion; and

f. Whether the Defendants' conduct constitutes unjust enrichment.

107. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class in that Plaintiff and the members of the Class sustained damages arising out of Defendants' uniform wrongful conduct.

108. **Adequate Representation**: Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff. Plaintiff and his counsel

are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

109. **Superiority**: This class action is also appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION
Violation of the Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505
(On Behalf of Plaintiff and the Class as Against Defendant University of Chicago)

110. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

111. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505 ("ICFA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

112. The ICFA prohibits any unlawful, unfair, or fraudulent business acts or practices,

including the employment of any deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of any material fact.

113. As described herein, the University has engaged in unlawful conduct and *per se* violations of the ICFA, as well as deceptive and unfair conduct.

114. Through its Notice of Privacy Practices and Admission and Outpatient Agreement and Authorization, the University represented to Plaintiff and the Class that it would, *inter alia*: protect their medical information, maintain the privacy of their medical information, follow the terms of the Notice of Privacy Practices in keeping their medical information confidential, and comply with any other federal and state laws, including all laws that govern patient confidentiality.

115. The University's privacy promises were, in fact, false. The University did not keep Plaintiff's and Class members' medical records confidential and did not prevent unauthorized access to them. In fact, the University did the opposite. On information and belief, Plaintiff's and the Class members' medical records were provided to Defendant Google when the University transferred hundreds of thousands of its patients' medical records to Defendant Google.

116. Knowing that consumers are less likely to do business with companies that fail to keep their personal information confidential, the University made the false privacy representations with the intention that Plaintiff would rely on them in contracting with the University for medical services.

117. Had the University disclosed that it would not keep Plaintiff's and the Class members' medical information confidential and, instead, provide it to Defendant Google—which did not comply with state and federal law—Plaintiff and the Class members would not have paid

at all for the University's health care services (*i.e.*, the value of health care services *without* adequate privacy protections is worth substantially less than the value of such services *with* adequate protections).

118. Accordingly, the University's false representations regarding its privacy practices constituted deceptive conduct prohibited by the ICFA.

119. The University's failures to comply with its privacy promises and obligations were also unlawful conduct prohibited by the ICFA.

120. The University's inadequate privacy protections violated state and federal law and are therefore unlawful under the ICFA.

121. The University's unlawful conduct caused Plaintiff and the Class members monetary damages because had the University disclosed that it would provide Defendant Google their medical records, they would not have paid at all for the University's health care services—either directly or indirectly by paying their health care insurance premiums, co-pays, and/or insurance deductibles.

122. Further, because Plaintiff and the Class members paid, in part, for the University to keep their medical information confidential in compliance with all relevant federal and state laws protecting and governing his medical information, they did not receive the services they paid for.

123. The University's deceptive, unlawful, and unfair conduct occurred in the course of consumers contracting for medical treatment, and therefore occurred in the course of conduct involving trade and commerce.

124. In sum, the University's deceptive, unlawful, and unfair conduct caused Plaintiff and the Class members monetary damage. They would have not paid for the University's health

care services had they known that the University would not keep their medical records private and confidential, in violation of the University's representations, and state and federal law.

125. Further, Plaintiff and the Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotion distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Breach of Express Contract
(On Behalf of Plaintiff and the Class as Against Defendant University of Chicago)

126. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

127. Plaintiff and the Class members entered into a valid and enforceable agreement with Defendant the University whereby the University promised to provide health care services to Plaintiff and the Class, and Plaintiff and the Class agreed to pay money for such services.

128. A material part of the University's promise to Plaintiff and the Class to provide health care services was to keep their medical information private and confidential in accordance with its Notice of Privacy Practices and Admission and Outpatient Agreement and Authorization.

129. In its written services contracts, patients' rights statements, and privacy policies, the University expressly promised Plaintiff and the Class that it would comply with all HIPAA standards, protect Plaintiff's and the Class members' medical information, and keep it confidential in accordance with its Notice of Privacy Practices, Admission and Outpatient Agreement and Authorization, and HIPAA.

130. The contracts required Defendant the University to safeguard Plaintiff's and the Class members' medical information, and keep it private and confidential.

131. A meeting of the minds occurred, as Plaintiff and the Class agreed, *inter alia*, to

provide accurate personal and family health information and to pay—either directly or indirectly by paying their health care insurance premiums, co-pays, and/or insurance deductibles—the University in exchange for the University's agreement to, among other things, protect her medical information.

132. Plaintiff and the Class fully performed their obligations under the contracts.

133. Defendant the University did not keep Plaintiff's and the Class members' medical information private or confidential when, on information and belief, it disclosed their medical records to Defendant Google.

134. The failure to meet these promises and obligations constitutes an express breach of contract. In other words, the University breached its contracts with Plaintiff and the Class by failing to keep their medical information private and confidential as described herein.

135. The University's failure to fulfill its promises resulted in Plaintiff and the Class receiving services that were of less value than he paid for.

136. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive—even though such protections were a material part of her contracts with the University—they did not receive the full benefit of the bargain.

137. As a result of the University's breach, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for the University's services as promised and the actual diminished value of its health care services.

138. Further, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(in the alternative to Count Two)
(On Behalf of Plaintiff and the Class as Against Defendant University of Chicago)

139. Plaintiff incorporates the foregoing allegation as if fully set forth herein.

140. In order to benefit from the University's services, Plaintiff and the Class were required to disclose medical information to the University, including their names, contact information (address, phone and fax numbers, and email address), Social Security Numbers, dates of birth, and extremely sensitive medical information.

141. By providing that medical information, and upon the University's acceptance of such information, Plaintiff and the Class members, on the one hand, and the University, on the other hand, entered into implied contracts whereby the University was obligated to take reasonable steps to keep that information private and confidential, as promised by its Notice of Privacy Practices, and Admission and Outpatient Agreement and Authorization.

142. A meeting of the minds occurred, as Plaintiff and the Class members agreed, *inter alia*, to provide their medical information and to pay—either directly or indirectly by paying their health care insurance premiums, co-pays, and/or insurance deductibles—the University in exchange for the University's agreement to, among other things, provide medical care and keep Plaintiff's and the Class members' medical information private.

143. Plaintiff and the Class members fully performed their obligations under the contracts.

144. Without such implied contracts, Plaintiff and the Class would not have provided their medical information to the University.

145. As described herein, the University did not keep Plaintiff's and the Class members' medical information private or confidential.

146. Because the University provided Plaintiff's and the Class members' medical information to Defendant Google, the University breached its implied contracts with Plaintiff and the Class.

147. The failure to meet its promises and obligations constitutes a breach of contract. In other words, the University breached its contracts by failing to keep Plaintiff's and the Class members' medical information confidential, as described herein.

148. The University's failure to fulfill its promises resulted in Plaintiff and the Class receiving services that were of less value than they paid for.

149. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive—even though such protections were a material part of the contracts with the University—Plaintiff and the Class did not receive the full benefit of the bargain.

150. As a result of the University's breach, Plaintiff and the Class members suffered damages in the amount of the difference between the price they paid for the University's services as promised and the actual diminished value of its health care services.

151. Further, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Tortious Interference with Contract
(On Behalf of Plaintiff and the Class as Against Defendant Google)

152. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

153. Plaintiff and the Class members entered into a valid and enforceable agreement with Defendant the University whereby the University promised to provide health care services to Plaintiff and the Class, and Plaintiff and the Class agreed to pay money for such services.

154. A material part of the University's promise to Plaintiff and the Class to provide health care services was to keep their medical information private and confidential in accordance with its Notice of Privacy Practices and Admission and Outpatient Agreement and Authorization.

155. In its written services contracts, patients' rights statements, and privacy policies, the University expressly promised Plaintiff and the Class that it would comply with all HIPAA standards, protect Plaintiff's and the Class members' medical information, and keep it confidential in accordance with its Notice of Privacy Practices, Admission and Outpatient Agreement and Authorization, and HIPAA.

156. The contracts required Defendant the University to safeguard Plaintiff's and the Class members' medical information, and keep it private and confidential.

157. Defendant Google had actual or constructive knowledge of Plaintiff's and the Class members' contracts.

158. Google intentionally and without justification interfered with the University's contracts with its patients—like Plaintiff and the Class members—with respect to keeping their medical information safe and private.

159. As a result of the University's breach, Plaintiff and the Class members suffered damages in the amount of the difference between the price they paid for the University's services as promised and the actual diminished value of its health care services.

160. Further, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class as Against Defendants)

161. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

162. Defendants intentionally intruded upon Plaintiff's and each of the Class members' seclusion by transmitting, receiving, examining, and analyzing patients' confidential electronic health records and using them for commercial purposes.

163. Defendants' transmission and receipt of patients' medical records is highly offensive to a reasonable person as it reveals intimate private details about their medical histories —such as chronic conditions, life-threatening illnesses, whether a person has addiction issues, disabilities, and issues related to pregnancy, along with personal details such as sexual preferences, gender nonconformity, and sexually transmitted diseases—and that they believed were confidential.

164. Defendants' intrusion upon the Plaintiff's and the Class members' seclusion caused Plaintiff and the Class members mental anguish and suffering in the form of anxiety and concern for the safety of their medical records.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class as Against Defendant Google)

165. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

166. Plaintiff and the Class members conferred a benefit on Google in the form of valuable confidential medical records it received from the University.

167. Defendant Google appreciates or has knowledge of the benefits conferred upon it by Plaintiff and the Class members.

168. Under principles of equity and good conscience, the Defendant Google should not

be permitted to retain any money derived from its acquisition of medical records, or the medical records themselves belonging to Plaintiff and the Class members, because it does not have authorization to possess or use those records.

SEVENTH CAUSE OF ACTION
Unjust Enrichment
(*In the Alternative to Count Two*)
(On Behalf of Plaintiff and the Class as Against Defendant the University)

169. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

170. Plaintiff and the Class members conferred a benefit on the University in the form of fees paid for health services.

171. Defendant the University appreciates or has knowledge of the benefits conferred upon it by Plaintiff and the Class members.

172. Under principles of equity and good conscience, Defendant the University should not be permitted to retain any money derived from its provision of medical records to Google because it did not have authorization to give those records to Google.

173. Had Plaintiff and members of the Class been aware that the University was going to share their medical records with Google, they would have paid less for their health care services, or not paid for services at the University at all.

174. Accordingly, as a result of Defendant the University's conduct, Plaintiff and the Class members suffered damages in the amount of the difference between the price they paid for the University's services as promised and the actual diminished value of the health care services they received.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Matt Dinerstein, individually and on behalf of a Class of similarly situated individuals, prays for the following relief:

a) An order certifying the Class as defined above, appointing Plaintiff Dinerstein as the representative of the Class, and appointing his counsel as Class Counsel;

b) An order declaring that Defendant University of Chicago's actions, as set out above, constitute a violation of the ICFA, a breach of express contract, a breach of implied contract, intrusion upon seclusion, and unjust enrichment;

c) An order declaring that Defendant Google's actions, as set out above, constitute tortious interference with contract, intrusion upon seclusion, and unjust enrichment;

d) An injunction requiring University of Chicago to comply with all HIPAA de-identification regulations and enjoining University of Chicago from disclosing identifiable patient medical records to third parties without first obtaining consent;

e) An injunction prohibiting Google from using patient records obtained from University of Chicago;

f) An order requiring Google to delete all patient records received from University of Chicago;

g) An award of actual damages; and

h) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can so be tried.

Respectfully submitted,

MATT DINERSTEIN, individually and on behalf of all other similarly situated,

Dated: June 26, 2019

By: /s/Jay Edelson
One of Plaintiff's Attorneys

Jay Edelson
jedelson@edelson.com
Benjamin H. Richman
brichman@edelson.com
Christopher L. Dore
cdore@edelson.com
J. Eli Wade-Scott
ewadescott@edelson.com
Michael W. Ovca
movca@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378