UNITED STATES DISTRICT COURT
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, THE UNIVERSITY OF CHICAGO MEDICAL CENTER, an Illinois not-for-profit corporation, and THE UNIVERSITY OF CHICAGO, an Illinois not-for-profit corporation,	)	**No. 19 C 4311**
Defendants.	)	**Judge Rebecca R. Pallmeyer**

MEMORANDUM OPINION AND ORDER

In 2017, Defendants The University of Chicago and The University of Chicago Medical Center (collectively "the University") and Google began a research partnership in which they used machine-learning techniques to create predictive health models aimed at reducing hospital readmissions and anticipating future medical events. As part of this research, the University disclosed to Google the "de-identified" electronic health records of all adult patients treated at its hospital from January 1, 2010 through June 30, 2016. Plaintiff Matt Dinerstein was an inpatient at the University in June 2015 and, asserting a variety of state-law claims, brings this suit pursuant to the Class Action Fairness Act ("CAFA") on behalf of all patients whose medical information was disclosed for Defendants' research. The University and Google have both filed motions to dismiss [43, 45]. In addition, the University has moved to strike the class allegations [49]. For the following reasons, Defendants' motions to dismiss are granted, and the University's motion to strike is terminated as moot.

BACKGROUND

The amended class action complaint ("AC") [42] alleges the following facts, assumed true for the purposes of this analysis. Plaintiff Matt Dinerstein had two separate hospital stays as a patient at the University's hospital in June 2015. (AC ¶ 98.) Each stay lasted for a few days (*id.*)

and Plaintiff paid premiums and other fees to health insurers who provided coverage for the treatment and services he received. (*Id.* ¶ 98.) During his stays at the hospital and throughout 2015, Mr. Dinerstein maintained an account with Defendant Google and used a smartphone with Google applications on it, which, he alleges, collected and transmitted to Google his geolocation information. (*Id.* ¶ 94.) Also during these stays, the University generated and maintained health records for Plaintiff, which included such sensitive information as his demographic data, vital signs, diagnoses, procedures, and prescriptions. (*Id.* ¶ 93.) Mr. Dinerstein received two forms relevant to this sensitive information: the Admission and Outpatient Agreement and Authorization form, and the Notice of Privacy Practices. (*Id.* ¶ 61.)

The Admission and Outpatient Agreement and Authorization ("the Authorization"), a copy of which was attached as an exhibit to the amended complaint, contains two paragraphs relevant to the present dispute:

> I understand and agree that my medical information in any form and any tissue, fluids, cells and other specimens that may be collected during this hospitalization and/or period of treatment may be used and shared for research that has been approved by the University of Chicago Institutional Review Board (IRB) and that has been found to pose a minimal risk. I acknowledge that such research by the University of Chicago Medical Center may have commercial value and, in that event, I understand that I will not be entitled to any compensation, regardless of the value of such research or any products or inventions developed therefrom.
>
> I understand that all efforts will be made to protect my privacy and that any use of my medical information will be in compliance with federal and state laws, including all laws that govern patient confidentiality, and the University of Chicago Medical Center Notice of Privacy Practices. I further understand that my identity and the identity of my medical records will not be included in any research findings or reports.

(Outpatient Agreement & Authorization § III, Ex. 2 to AC [42-2].) *See* FED. R. CIV. P. 10(c) ("A copy of a written instrument that is an exhibit to a pleading is a part of the pleading for all purposes.").

The Notice of Privacy Practices ("the NPP") contains the following provisions that are also important to the instant case:

> We respect the privacy of your medical information. Each time you visit us, we record information about the care you receive, including external information we

> receive about your health care and information to seek payment for our services (your "medical information"). This medical information is also called your "Protected Health Information") ("PHI"). These records may be kept on paper, electronically on a computer, or stored by other media.
>
> [The University Chicago Medical Center ("UCMC")] is required by law to:
>
> - Maintain the privacy and security of your PHI;
> - Notify you following a breach of your unsecured PHI, if required by law;
> - Provide this Notice to you and describe the ways we may use and share your PHI;
> - Notify you of your rights regarding your PHI;
> - Follow the terms of this Notice.
>
> . . .
>
> We perform research at UCMC. Our researchers may use or share your information without your authorization (a) if the group that oversees research gives them permission to do so, (b) if the patient data is being used to prepare for a research study, or (c) if the research is limited to data of deceased patients.
>
> . . .
>
> We will not use or share your medical information for any reason other than those described in this Notice without a written authorization signed by you or your personal representative. An authorization is a document that you sign that directs us to use or disclose specific information for a specific purpose. . . .
> We will obtain your written permission:
>
> . . .
>
> - For the sale of your medical information.

(NPP at 1–2, 4, 5, Ex. 1 to Univ. Mem. in Supp. of Mot. to Dismiss [44-1].)[1]

In May 2017, Google announced that it had partnered with the University to use "machine learning" to identify patients' health problems and predict future medical events. (AC ¶ 58.) To conduct this study, the University transferred electronic health records ("EHRs") to Google. (*Id.* ¶ 59.) This transfer was made pursuant to a December 2016 Data Use Agreement ("DUA") under which the University would transfer to Google the EHRs of every patient, age eighteen or older,

[1] Unlike the Authorization, Plaintiff did not include the NPP as an exhibit to the amended complaint. The court may nevertheless consider the document as part of the pleadings because Plaintiff referred to it in the amended complaint and the University has included it with the motion to dismiss. *See Feigl v. Ecolab, Inc.*, 280 F. Supp. 2d 846, 848–49 (N.D. Ill. 2003).

who used the University's outpatient, inpatient, or emergency services between January 1, 2010 and June 30, 2016. (*Id.* ¶ 66; *see* DUA at 9, Ex. 1 to AC [42-1].) Google has submitted a patent application for a system that aggregates EHR data and uses machine learning on those records to predict future medical events. (AC ¶ 54.) The patent application's abstract further describes the invention as providing an interface for healthcare providers to see past and predicted future medical events for a patient. *See* U.S. Patent Publication No. US2019/0034591. According to the amended complaint, by submitting the patent application in 2017, Google "demonstrat[ed] its clear intent to commercialize the University's medical records prior to obtaining them." (AC ¶ 54.)

Plaintiff alleges that while Google retains all rights to the software created using the EHRs, the DUA granted the University a perpetual license to use that software. (*Id.* ¶ 66.) Google disputes this characterization of the DUA. (Google Mem. in Supp. of Mot. to Dismiss [46] at 3 n.3.) In fact, it is not apparent to the court what exactly has been granted to the University. *See Bytska v. Swiss Int'l Air Lines, Ltd.*, No. 15 C 483, 2016 WL 792314, at *3 (N.D. Ill. Mar. 1, 2016) (explaining that if "an exhibit incontrovertibly contradicts the allegations in the complaint, the exhibit ordinarily controls, even when considering a motion to dismiss"). The DUA grants to the University, "for internal non-commercial research purposes," "a nonexclusive, perpetual license to use the [ ] Trained Models and Predictions" created by Google. (DUA § 3.12.) The Trained Model refers to the model created via machine learning conducted on the EHRs, and Predictions are the results of the model's computations. Specifically, the DUA defines "Trained Model" as "the Model parameters arranged in accordance with the Model's mathematical form," which are determined by using "the Limited Data Set"—the EHRs disclosed by the University to Google—"as Input Data" to "train" the Model. (*Id.* § 1.12.) Training a model means "using Model Software to create Model parameters for a Model form using Input Data." (*Id.* § 1.12.) And the "Model Software" is "used to Train a Model and compute Predictions," (*id.* § 1.7), where "Predictions" are the outputs "of a Model for a given set of Input Data." (*Id.* § 1.6.)

In early 2018, Defendants published a study discussing the results of their research and methodology. (AC ¶ 64; *see* Alvin Rajkomar et al., *Scalable and Accurate Deep Learning with Electronic Health Records*, 1 NPJ Digital Media (January 2018), https://www.nature.com /articles/s41746-018-0029-1 (last visited Sept. 1, 2020).) The article explains that the study used EHRs provided by Defendant University and the University of California, San Francisco ("UCSF") that included the following "de-identified" information: "patient demographics, provider orders, diagnoses, procedures, medications, laboratory values, vital signs, and flowsheet data . . . from all inpatient and outpatient encounters." (Rajkomar et al., *Scalable and Accurate Deep Learning* at 6.) The article notes that Defendant University—but not UCSF—included the "dates of service" as well as "free-text medical notes" in the EHRs provided to Google. (*Id.*) According to Plaintiff, disclosing such information is a *prima facie* violation of the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996). (AC ¶ 67.) These records were not, the amended complaint alleges, sufficiently anonymized, and therefore put patient privacy at risk. (*Id.* ¶ 68.) The amended complaint points out that at a 2017 conference hosted by Google, the University's Associate Chief Research Informatics Officer himself said that protecting patient anonymity in free-text notes requires not only making certain redactions but actually changing information like a patient's age and other biographical information. (*Id.* ¶ 69.) Yet the parties' DUA provides that the University would share patients' ages with Google. (*Id.*) And the free-text notes shared with Google are alleged to have not been sufficiently redacted or anonymized. (*Id.*) Plaintiff claims that free-text notes "are normally not included in de-identified medical records," and also "create an enormous wealth of data re-identifying the patients themselves." (*Id.* ¶ 88.) According to the amended complaint, whatever process was used to redact these notes was not properly audited or independently verified. (*Id.* ¶ 89.)

These disclosures, Plaintiff alleges, violate HIPAA because the University either did not make an expert determination that the risk of re-identifying the data was very small or, if such a

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.