+
WHITE PAPER

+
CATALYSTS DRIVING SUCCESSFUL DECISIONS IN LIFE SCIENCES

PROTECTING PRIVACY IN THE AGE OF PATIENT CENTRICITY

by
JESSICA SANTOS, PH.D.

JULY 2016

KANTAR HEALTH

+
EVERY EU CITIZEN IS COVERED BY PRIVACY LAWS IN ALL CIRCUMSTANCES, NOT JUST WHEN THEY ARE USING THE HEALTHCARE SYSTEM.

The healthcare industry's focus on patient centricity has meant that healthcare researchers working on behalf of the industry are looking for patient insights through a variety of channels – from healthcare providers, from the patients themselves and from biometric data, to name just a few. However, researchers face many challenges in protecting patients' privacy: the copious amount of data being collected; the difficulty in keeping patient data absolutely anonymous at all times; the possibility of discovering patient information that the patients themselves are unaware of, such as from genomic sequencing; and the industry as a whole working on innovations that will change diagnosis, treatment and resource allocation that will be a potential minefield for privacy regulations.

The healthcare industry has numerous rules in place to protect patients' privacy and healthcare information. For example, in Europe this information is protected by the General Data Protection Regulation (GDPR), while U.S. patients are covered by the Health Insurance Portability and Accountability Act (HIPAA), and most countries place healthcare information in the sensitive or special category in their legislations. Healthcare researchers need to understand these guidelines and how to protect individuals' privacy.

GDPR: GIVING EU CITIZENS CONTROL

Privacy is an overarching concern in Europe; everyone is covered by privacy laws in all circumstances, not just when they are using the healthcare system. Europeans are protected by the GDPR,[1] which is a regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repeals EU Directive 95/46/EC.[2] It will come into effect in the spring of 2018.

The GDPR will impose new obligations on organizations that process the personal data of European Union residents. It is a general regulation designed to give citizens more control over their own private information in a digitized world of smartphones, social media, internet banking and global transfers, and also sets minimum standards on use of data for policing and judicial purposes.

Research is clearly defined within the GDPR. The GDPR adopts a "broad" definition of research, encompassing the activities of public and private entities alike (Recital 126). In the age of big data, where the data analytics activities of many organizations may qualify as research,[3] it is unclear exactly how far the GDPR's research exemption will extend. One thing is clear, however: The GDPR aims to encourage innovation, as long as organizations implement the appropriate safeguards.

While research in general enjoys the wider acceptance of GDPR, research involving healthcare data still needs explicit consent. The GDPR forbids a controller from processing "special categories of data" – sensitive data revealing racial or ethnic origin, religious or political beliefs, as well as genetic, biometric and health data – except in certain enumerated circumstances, such as where the data subject provides "explicit consent" or where the data was "manifestly made public by the data subject" (Article 9(2)(a); Article 9(2)(e)).

The research exemptions apply to processing personal data for scientific and historical research, statistical research, and archiving in the public interest. The recitals treat each

+
PROTECTION OF PATIENT INFORMATION IN THE U.S. FALLS AWAY FROM HIPAA WHEN THE PATIENT VOLUNTARILY SHARES THEIR DATA.

type of research separately. Healthcare research is included in the category of scientific research.

Scientific research is defined "in a broad manner" (Recital 126). The recital supplies examples, such as "technological development and demonstration, fundamental research, applied research, privately funded research," as well as public health research. The recital cites Article 179(1) of the Treaty on the Functioning of the European Union, which promotes "the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely." This suggests that although private research for technological development qualifies as research, the research may be required to be published or otherwise made available outside the private entity. An important interpretative question concerns the application of the research provisions to corporate contexts such as research for product improvement or marketing purposes, as opposed to "Big R" research in academic institutions, which is geared at publication and contribution to generalizable knowledge.

HIPAA: HOW EFFECTIVE IS IT?

Patients in the United States are not protected by an overarching privacy law like European patients are, but they do have HIPAA[4] legislation to protect their healthcare data. Originally enacted in 1996, HIPAA principally consists of the Privacy Rule and the Security Rule. It covers protected health information (PHI) that is disclosed by patients to covered entities,[5] which include healthcare providers, health plans and health insurance companies, and healthcare clearinghouses, such as billing services. Business associates[6] – defined as any organization or person working in association with or providing services to a covered entity that handles or discloses PHI – and their subcontractors are now also covered. Any research firms that receive PHI from covered entities are considered as business associates.

HIPAA violations are not uncommon. In 2014 – the most recent year for which data is available – 17,779 health information privacy complaints were received, up 37% from the previous year.[7] The violations fall under both the Privacy Rule and the Security Rule. The Privacy Rule establishes national standards for the protection of certain health information. The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.[8] Types of violations can include IT breaches in which hackers target healthcare data, accidental disclosure in which PHI is disclosed to a person who is not authorized the access it, and data not being processed properly.

HIPAA Is Not Inclusive

Data privacy laws in the U.S. pose one large discrepancy. While healthcare information is protected under HIPAA, that protection falls away when data are self-reported by the patient, such as when a person participates in an online survey or voluntarily shares data online or via social media. Because the U.S. does not have an overarching privacy law like

the EU, practitioners handling self-reported patient data often turn to FTC Act section 5[9] as their guideline legislation.

HIPAA Identifiers

The data collected through electronic medical records (EMR) or through HIPAA platform are very powerful. Researchers can use the data in EMRs, as long as the data are de-identified (see sidebar). HIPAA very clearly covers 18 identifiers; as long as all 18 and they have been removed from a dataset, it is considered a de-identified dataset and can be used for research purposes. Another option is to have a qualified statistician determine that the risk is very small that the information could be used to identify the individual.

However, even without using the 18 HIPAA identifiers data can still be used to identify people. Analysts can use more sophisticated algorithms to determine, for example, which group of people has higher risk to increase insurance premiums. While this would be considered a violation of the basic right to privacy in Europe, privacy laws in the United States would not protect against this sort of data usage.

OTHER AGENCIES WORKING TO PROTECT PATIENTS' PRIVACY

In the United States data privacy is overseen by the Federal Trade Commission (FTC). In 2012 the agency released a report setting forth best practices for businesses to follow to protect consumers' privacy and give them better control over the collection and use of their personal data. The recommendations include:

+ Privacy by Design: Companies should build in consumers' privacy protections at every stage in developing their products.
+ Simplified Choice for Businesses and Consumers: Companies should give consumers the option to decide what information is shared about them, and with whom.
+ Greater Transparency: Companies should disclose details about their collection and use of consumers' information, and provide consumers access to the data collected about them.[11]

In addition to the GDPR, data privacy in Europe is overseen by individual countries' data protection authorities (DPA). These agencies have a more active role in looking after patient privacy and are independent, public authorities that are responsible for monitoring the application of data protection laws within its territory. DPAs have the power to investigate data breaches, intervene before operations are carried out, engage in legal proceedings when national provisions have been violated, and hear claims regarding the protection of personal data rights.[12] European DPAs include the UK's Information Commissioner's Office (ICO), France's *La Commission nationale de l'informatique et des libertés* (CNIL) and Germany's *Bundesdatenschutzgesetz* (BDSG).

At a more local level, hospitals often employ an ethics committee or an ethics consultant to advocate for patients and their privacy. Traditionally the ethics committee works to promote the rights of patients and encourage shared decision making between patients

18 HIPAA IDENTIFIERS[10]

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 a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000

C. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; 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

E. Fax numbers

F. Electronic mail addresses

G. Social security numbers

H. Medical record numbers

I. Health plan beneficiary numbers

J. Account numbers

K. Certificate/license numbers

L. Vehicle identifiers and serial numbers, including license plate numbers

M. Device identifiers and serial numbers

N. Web Universal Resource Locators (URLs)

O. Internet Protocol (IP) address numbers;

P. Biometric identifiers, including finger and voice prints

Q. Full face photographic images and any comparable images

R. Any other unique identifying number, characteristic, or code

+
THE INCREASING FOCUS ON PRIVACY HAS MADE HEALTHCARE PRACTITIONERS MORE RELUCTANT TO PARTICIPATE IN PATIENT RESEARCH.

(or their surrogate) and the physician. However, committee members are also on hand to address issues of patient privacy or confidentiality.[13]

HOW DO THESE RULES AFFECT HEALTHCARE RESEARCHERS?

Patient-centric research doesn't only mean research directly with patients and other healthcare consumers. It also includes asking healthcare providers to release patient information, either via patient records, aggregated data or anecdotal data. The increasing focus on patient privacy has made healthcare practitioners more reluctant to release patient data, and many doctors are confused by what they can and cannot release. In response, doctors will sometimes only talk about aggregated patient information, and some will not participate in any survey that deals with patients rather than inadvertently releasing patient information.

Two solutions exist for using individual patient data for analysis. One solution is to get the study classified as real-world research. Real-world research encompasses many types of information, including claims data, clinical trial data, data from electronic health records, pharmacy data, and data collected directly from the patient. These data typically conform to privacy regulations because studies that collect real-world evidence are subject to approval and oversight from an Institutional Review Board (IRB) or an ethics committee approval.

The second solution is a syndicated study. These studies have no sponsor, and an agency is completely responsible for collecting and analyzing data and ultimately sells aggregated reports. That will reduce the risk of the sponsor and healthcare provider violating individual patient data and patient privacy.

The best way to ensure a patient's privacy isn't being violated is to receive their consent, offering them the ability opt-in or opt-out of having their information shared. However, there is some disagreement about whether patients understand what they are giving consent to. After all, privacy policies and terms & conditions documents are often quite lengthy and not written in layman's terms. Therefore, GDPR is no longer considering consent as the "waterproof" mechanism for data processing, and the U.S. Department of Health and Human Services encourages healthcare providers and researchers to adequately inform patients of how their data will be use so patients can make a "meaningful" consent choice.[14] Agency's privacy by design (PbD) infrastructure, industry reputation, onward transfer limitation, detailed privacy policy and protection commitment are all essential elements to gain trust from both HCPs and sponsors.

+ REFERENCES

1. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1462359521758&from=EN

2. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012

3. https://bigdata.fpf.org/wp-content/uploads/2015/12/Tene-Polonetsky-Beyond-IRBsEthical-Guidelines-for-Data-Research1.pdf

4. http://www.hhs.gov/hipaa/

5. http://www.hhs.gov/hipaa/for-professionals/covered-entities/

6. http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

7. Office for Civil Rights. U.S. Department of Health & Human Services. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html. Accessed 24 Jun 2016.

8. Summary of the HIPAA Security Rule. Office for Civil Rights. U.S. Department of Health & Human Services. http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/. Accessed 24 Jun 2016.

9. https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf

10. www.hhs.gov/ocr/privacy/index.html Aug 2009, Summary of the HIPAA Privacy Rule, U.S. Department of Health & Human Services, edocket.access.gpo.gov/cfr_2002/octqtr/pdf/45cfr164.514.pdf Aug 2009

11. FTC Issues Final Commission Report on Protecting Consumer Privacy. FTC.gov. https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy. Accessed 29 Jun 2016.

12. Data protection authority. IT Law Wiki. http://itlaw.wikia.com/wiki/Data_protection_authority. Accessed 29 Jun 2016.

13. Ethics Committees, Programs and Consultation. Ethics in Medicine. University of Washington School of Medicine. https://depts.washington.edu/bioethx/topics/ethics.html. Accessed 29 Jun 2016.

14. Patient Consent for eHIE. HealthIT.gov. https://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy. Accessed 28 Jun 2016.

+

ABOUT THE AUTHOR

JESSICA SANTOS, PH.D.

Dr. Jessica Santos is the Global Compliance and Quality Director at Kantar Health, the largest custom market research company focused on the life sciences industry. She is primarily responsible for providing oversight and support across the 40+ Kantar Health global offices in the areas of regulation, interaction with clients, suppliers and others within Kantar Health, Kantar and WPP. Dr. Santos is responsible for maintaining, anticipating and coordinating all activities with regard to compliance laws/regulations, industry guidelines, pharamcovigilance and client contracts, defining and driving the execution of Kantar Health's Quality Strategy – our approach to measuring and improving our quality efforts.

Dr. Santos is an experienced statistician, analyst, methodologist and market research scientist. She gained her reputation through her publications and professional committee work in the industry. She is a frequent speaker and contributor in major conferences and has a Ph.D. in Marketing, an MRS fellowship and Chartered Marketer status.

Dr. Santos is a member of UK Research Ethics Committee, EphMRA, BHBIA and PMRG Government Affairs Committee, reviewer and co-chair of ISPOR, and MRS Professional Development Advisory Board and Examiner.

+ WHY KANTAR HEALTH

Kantar Health is a leading global healthcare consulting firm and trusted advisor to many of the world's leading pharmaceutical, biotech and medical device and diagnostic companies. It combines evidence-based research capabilities with deep scientific, therapeutic and clinical knowledge, commercial development know-how, and brand and marketing expertise to help clients evaluate opportunities, launch products and maintain brand and market leadership. Our advisory services span three areas critical to bringing new medicines and pharmaceutical products to market – commercial development, clinical strategies and marketing effectiveness.

FOR MORE INFOMATION, PLEASE CONTACT:
INFO@KANTARHEALTH.COM