Risky Business?

Sharing Data with Entities Not Covered by HIPAA

ISSUE BRIEF
2019

manatt

eHEALTH INITIATIVE

Introduction

In 2018, eHealth Initiative Foundation (eHI) and Manatt, Phelps & Phillips hosted two executive advisory board meetings on privacy and security in the age of wearable technologies. The risky business of sharing data *In and Outside* of the healthcare system is becoming more complicated, especially as consumer use of health applications and the desire to share health data increases exponentially. The roundtables convened experts in healthcare privacy and security and explored data sharing within and between organizations, including the relationships healthcare providers have with business associates and application (app) developers. The roundtables also tackled data sharing implications for the bio-economy and the state, federal, and international policies and rules that aim to guide organizations through the murky terrain.

Current privacy laws were not created during the age of technology, big data, and mobile healthcare (mHealth). One of the most critical pieces of privacy legislation, the Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, during a time when healthcare providers and payers used paper-based medical records to maintain health information, instead of electronic health records (EHR). The iPhone, iPad, and other mobile devices did not emerge until almost a decade later. While HIPAA was amended in the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act to address concerns arising from the use of EHRs, numerous challenges remain with the aging legislation. A significant amount of health data is now generated from healthcare apps and consumer devices that are ungoverned by HIPAA. As corporate entrants to the healthcare industry increase, confusion about the handling of health information by app developers abounds.

Covered Vs Non-Covered HIPAA Entities

Organizations that are legally required to follow the privacy and security rules laid out in HIPAA are called "covered entities". Typically, covered entities are health plans, healthcare clearinghouses, and providers conducting HIPAA transactions. Protected health information (PHI) found in medical records, claims information, and lab results is covered under HIPAA. Certain organizations that conduct business with covered entities also need to follow HIPAA. These "business associates" are required to sign a "business associate agreement" with the covered entity and must comply with HIPAA security and privacy standards.

With business associates, if breaches of app data occur, breach notification, pursuant to HIPAA, is also required. Covered entities have numerous issues to consider before working with vendors, providers, and subcontractors who might come into contact with PHI. In today's world of mHealth, web portals, and smart phones, covered entities are struggling to understand the parameters for identifying and working with app developers that may or may not constitute business associates. When covered entities decide to partner with app developers, determining if the app developer is a business associate is extremely important as it sets the stage for whether or not the data shared by the covered entity with the app developer is regulated under HIPAA.

DETERMINING WHO IS A BUSINESS ASSOCIATE

HIPAA-covered entities, such as payers and healthcare providers, are often involved with organizations that rely on health data as an element of their commercial activity, including data brokers, advertisers, websites, marketers, genetic testing companies, and others. Unfortunately, determining if these organizations are business associates can be complicated. At the heart of the business associate determination is whether the app is being offered *on behalf of the covered entity*. Various factors contribute to the business associate determination:

- How is the app branded?
- Do consumers access the app through the covered entity or a separate channel?
- Is the app (or an enhanced version) available only through the covered entity, for example only to patients or members of the covered entity?
- How does the data flow between the covered entity and app developer?
- Does the app developer provide any related services to the covered entity?

For example, if a provider contracts with an app developer for patient management services—including remote patient health counseling; monitoring of patients' food and exercise; patient messaging; EHR integration; and application interfaces that involve creating, receiving, maintaining, and transmitting PHI—and the app is a means for providing those services, the app developer is likely a business associate and a business associate agreement is required. In this scenario, the patient downloads the health app to his or her phone at the direction of the provider, and information the patient enters is automatically incorporated into the EHR.

In another example, if a consumer downloads an app, offered by his or her health plan, that provides the capability to request, download, and store plan records, and check the status of claims, the covered entity likely needs a business associate agreement with the developer. The health plan would have commissioned the creation of the app, which may also contain the plan's wellness tools and analyze app data to evaluate the effectiveness of the wellness program.

BUSINESS ASSOCIATES

An entity that creates, receives, maintains, or transmits Protected Health Information (PHI) "on behalf of" or to provide services to a covered entity. Expressly includes an entity transmitting PHI that requires routine access and an entity offering personal health records on behalf of the covered entity.

Understanding Protected Health Information

In the last several years, many new non-covered HIPAA businesses are entering the health IT industry and are dependent upon PHI for their success. PHI is difficult and expensive for app developers, artificial intelligence analysts, and other data miners to obtain. Therefore, payers and providers who control vast amounts of PHI are often courted by non-covered groups who want to commercialize and profit from PHI. In the absence of authorization by the subject of the PHI, PHI collected by app developers that are business associates of covered entities may only be used or disclosed for HIPAA-permitted purposes and as authorized in the business associate agreement. Such PHI must be returned to the covered entity or destroyed upon termination of relationship.

Consumers Acting on Their Own Are Not Business Associates

If a company offers a direct-to-consumer version of an app that is not provided on behalf of a covered entity, it is not subject to HIPAA. Any arrangement where a company provides an app or service directly to a consumer and transmits data *on behalf of the consumer* does **not** create a business associate relationship with a covered entity. For example, if a consumer downloads data from his or her doctor's EHR through a patient portal and then uploads the data into a health app that the provider has no role in developing, there is no business associate relationship between the organization offering the app and the provider. The provider did not hire the app developer to provide or facilitate the service.

Similarly, even if a provider and app developer have entered into an arrangement to facilitate an exchange of information between the EHR and app, if actions are taken *at the consumer's request,* there may not be a business associate relationship. In such a scenario, the consumer could download an app where they can access test results from the provider, populate data on the app, and direct the app to transmit data to the EHR. All actions could be done at the consumer's request; therefore, the app developer and covered entity most likely do not need a business associate agreement.

Federal Guidance & Regulations for Covered Entities & App Developers

In an effort to keep up with changing times, states, federal agencies, and countries are increasingly developing resources to deal with the evolving nature of technology in healthcare. In their attempts to bridge the technology gap with industry, federal government agencies are offering guidance for business associates and covered entities. Several pertinent regulations also exist. Knowing and adhering to regulations is important, as the Federal Trade Commission (FTC) will prosecute entities that fail to protect consumer data.

The HITECH Act permits State Attorneys General (AG) to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules. HITECH also gives AGs the authority to bring civil actions on behalf of state residents for violations. The Office of Civil Rights (OCR) developed HIPAA Enforcement Training to help AGs and their staffs use their new authority. The training course aids AGs in investigating and seeking damages for HIPAA violations that affect residents of their states. More enforcement of regulations is needed, and agencies are considering expanding the penalties for abuse. OCR receives reports of breaches and has been accepting complaints from individuals and employees since 2003. HITECH requires compliance reviews on all cases.

The Department of Health and Human Services' (HHS) Guidance on HIPAA & Cloud Computing, while intended for cloud computing, has also proven relevant for business associates and covered entities. This guidance presents eleven key questions and answers to assist HIPAA regulated Cloud Service Providers (CSPs) and their customers in understanding their responsibilities under the HIPAA Rules when they create, receive, maintain, or transmit electronic PHI (ePHI) using cloud products and services. The chart below provides links to these initiatives and others such as the 21st Century Cures Act and the Trusted Exchange Framework and Common Agreement (TEFCA), which are intended to bring healthcare innovation infrastructure into the 21st Century, and the eHealth Initiative created by the Centers for

Medicare & Medicaid Services (CMS) to simplify the adoption of electronic standards and health information technology.

The National Institutes of Health (NIH) created guidance for covered entities, businesses associates, and hybrid entities that perform both covered and noncovered functions as part of their business operations and the Food and Drug Administration (FDA) "recognizes the extensive variety of actual and potential functions of mobile apps, the rapid pace of innovation in mobile apps, and the potential benefits and risks to public health represented by these apps." In 2015, the expansion and broad applicability of mobile apps led the FDA to issue guidance that replaced their 2013 guidance, which informs manufacturers, distributors, and other entities about the subset of mobile app platforms and select software applications the FDA intends to apply their regulatory authority towards.

GUIDANCE & REGULATIONS FOR MOBILE APPS	
21st Century Cures Act	• https://energycommerce.house.gov/cures/
CMS	• https://www.cms.gov/eHealth • https://www.cms.gov/eHealth/downloads/eHealth-Fact-Sheet.pdf
FDA	• https://www.fda.gov/downloads/medicaldevices/.../ucm263366.pdf
FTC	• https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool • https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices
HIPAA Security Rule	• https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
HITECH Enforcement	• https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf
NIH	• https://privacyruleandresearch.nih.gov/pr_06.asp
TEFCA	• https://www.healthit.gov/sites/default/files/tefca2017oncannualmeetingfinal.pdf

Prosecuting HIPAA Violators

State AGs and the FTC have a record for prosecuting privacy breaches. In 2007, the Texas AG sued CVS/Caremark after finding customer records with personal information (names, addresses, dates of birth, driver licenses, types of medications prescribed, and credit card numbers with their expiration dates) in the trash cans behind one of the Texas locations of the drugstore chain. The FTC also opened an investigation and settled with CVS/Caremark on the charges that the company failed to protect medical and financial privacy of customers and employees. In 2009, the FTC approved a final consent order in the case. In a separate but related agreement, CVS Pharmacy paid $2.25 million to settle allegations of HIPAA violations.[i] In a more recent example, Practice Fusion settled with the FTC after charges that the cloud-based EHR vendor misled patients into sharing sensitive medical data without their knowledge that the information could be posted in a public-facing provider directory.[ii] Covered entities need to be particularly mindful of their business relationships with app developers as not to create mHealth breaches analogous to these cases.

[i] https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial

[ii] https://www.healthcareitnews.com/news/ehr-maker-practice-fusion-settles-ftc-over-patient-privacy-complaint

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) gives consumers the right to know how much of their personal data is being collected by companies, as well as the right to have that data deleted upon request. It was signed into law on June 28, 2018 and goes into effect in January 2020. The CCPA was added to the California code to provide core consumer rights as well as strong enforcement and stiff penalties for privacy breaches. In certain respects, the CCPA resembles the European Union's (EU) General Data Protection Regulation (GDPR), discussed in the next section.

Personal Information (PI) **(*defined by the CCPA*)**

Any information that could reasonably be linked to a consumer, including, but not limited to, personal identifiers, commercial information, biometric information, Internet activity information and employment information.

The CCPA is the nation's strictest consumer privacy and data protection measure. The law will apply to any for-profit entity doing business in California that (1) collects California residents' personal information (PI) solely or jointly with others, and (2) either (i) exceeds $25 million in annual gross revenues; (ii) annually transacts in the PI of 50,000 or more consumers, households, or devices; or (iii) derives half or more of its annual revenues from PI sales. The law applies to businesses that collect, use, or share PI of California residents, including those who are outside the state for temporary or transitory purposes (e.g., travelers).

Companies already regulated under either the California Confidentiality of Medical Information Act (CMIA) or HIPAA should continue to comply with those rules when handling medical information. The CCPA does not supersede those laws. A significant portion of California's hospitals are not-for-profit, which means they may not be subject to the CCPA at all. Although the law exempts businesses and providers covered by HIPAA, it will have an enormous impact on a wide range of consumer-directed healthcare companies, including those working with digital health, pharmaceutical and medical device manufacturers, healthcare technology companies, wearable manufacturers, and mHealth app developers. These companies collect large amounts of consumer healthcare data and are not covered by HIPAA. Given the breadth of information regulated by the CCPA, for-profit healthcare companies will still be subject to the CCPA requirements to the extent they gather or process PI, such as IP address, commercial information, internet activity, geolocation, employment-related information, education information, and "inferences" drawn from any such information to create a profile reflecting consumer characteristics.

The CCPA will require covered businesses to ensure an assortment of consumer rights and related notices that include:

- **Right of Access.** Consumers may request disclosure of the specific PI that a business has collected about the consumer.
- **Right of Deletion.** Consumers may request that a business delete any PI it has collected from the consumer and may direct any service providers to do the same, subject to several exceptions, such as when PI is needed to complete requested transactions or services.
- **Right to Know.** Consumers may request disclosure of the categories and specific pieces of PI collected about them, the sources from which the PI was collected, the purpose for such collection, and the categories of third parties the PI is shared with or sold to.
- **Right to Opt Out or Opt In.** Consumers may opt out of any sale of their PI to third parties, and consumers under age 16 must opt in to any such sales.

- **Right of Equal Service.** Covered businesses must not discriminate against consumers exercising any of the above rights, including through pricing and quality of goods or services, unless different treatment is reasonably related to the value provided to the consumer by his or her data. However, businesses may offer reasonable financial incentives related to PI collection, sale, or deletion.

Violating the CCPA

Under the state's Unfair Competition Law (UCL), violations of the CCPA provisions are actionable by the California AG after a 30-day cure period has passed. In addition to UCL penalties, the law authorizes civil penalties of up to $7,500 per violation. The CCPA also provides a limited private right of action for data breaches. The right of action has two major prerequisites: first, 30 days' written notice to the business identifying the allegations and an opportunity to cure, and second, notification to the AG within 30 days of filing a complaint, requiring the AG's response within 30 days that states whether the AG will prosecute the matter within six months and potentially whether the consumer is not authorized to proceed. Only once these preconditions are met may the consumer proceed with his or her civil claim for the greater of statutory damages between $100 and $750 per incident or actual damages and injunctive or declaratory relief.

GENERAL DATA PROTECTION REGULATION

The GDPR took effect on May 25, 2018 and replaced the 1995 EU Data Protection Directive as the framework governing the processing of personal data across EU member states. While U.S. privacy laws are mostly sector-based, the GDPR's approach is industry-agnostic and can be applied to any company in the world that processes the personal data of anyone physically located in the EU. The GDPR generally applies to "the processing of personal data," with a few exceptions. Several obligations apply, including the need to establish a legal basis for processing personal data and, if sensitive personal data is involved, the need to satisfy additional special conditions. The GDPR requires organizations' due diligence regarding their own activities, as well as those of business partners and vendors, in figuring out what is being collected, from whom and how.

Personal Data
(*defined by the GDPR)*

Broadly includes "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, culture or social identity of that natural person."

The GDPR is designed to harmonize data privacy laws across Europe and give greater protection and rights to individuals. In the regulation, there are 99 articles setting out the rights of individuals and obligations placed upon organizations. Eight rights for individuals allow easier access to the data companies hold on consumers. Companies covered by the GDPR are accountable for their handling of personal data, and those with more than 250 employees need to have documentation of why personal data is being collected and processed, descriptions of the information held, how long the data is kept, and descriptions of technical security measures in place. Additionally, companies that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data have to employ a data protection officer (DPO). Businesses are also required to use a "positive opt-in" process.

Violating the GDPR

Under the GDPR, the "destruction, loss, alteration, unauthorized disclosure of, or access to" consumer data has to be reported to a country's data protection regulator where it could have a detrimental impact on that person. It can include, but is not limited to, financial loss, confidentiality breaches, damage to reputation and more. The Information Commissioner's Office (ICO) and people impacted should be informed about a breach 72 hours after an organization finds out it has occurred. Organizations can be fined for security breaches, not processing personal data correctly, and not having a data protection officer.

IMPLICATIONS OF THE CCPA AND THE GDPR FOR INDUSTRY & CONSUMERS

Knowing what information is being gathered, for whom it is being collected, then asking the business case for the information, including if it is truly needed, will help companies with compliance for both for the GDPR and the CCPA. Although the CCPA helps California, it does not address larger, nationwide issues with privacy, security, and technology. Additionally, the GDPR was not crafted with the U.S. as a frame of reference. There has been no guidance on the GDPR and HIPAA interface. Entities conducting business overseas with U.S. consumers, however, still need to follow U.S. rules. Although the U.S. Government is behind the curve in creating comprehensive, national legislation that handles all aspects of consumer privacy and considers the technological advances of the future, each state mandating various privacy laws would be disastrous for consumers and stifling for industry.

Though healthcare companies are well acquainted with privacy and data security regulation, the CCPA introduces burdensome obligations, most of which were previously unseen by American companies and several of which present questions about implementation. Companies will have the right to cure alleged data breaches, but what constitutes a cure remains unstated. The GDPR may have its issues, but the fact Europe created a comprehensive standard is significant. Blockchain and cryptocurrency have increased the pace and nature of technology. In the absence of legislation, companies shop for the weakest links, which can lead to a host of ramifications for companies and consumers.

Discrepancies in breach notifications is one example of why a national solution is needed. Although companies have advocated for notification periods as long as 90 days, the CCPA requires breach notification to occur within five days and the GDPR requires notification within 72 hours. A national standard would alleviate the confusion. The National Association of Insurance Commissioners developed a consumer protection law[iii] that 12 states are considering, and over the course of six months, the Center for Democracy & Technology convened to create recommendations[iv] for a baseline privacy law the U.S. could follow. A national level standard would also make the flow of information easier.

[iii] Insurance Data Security Model Law, https://www.naic.org/store/free/MDL-668.pdf
[iv] Competition and Consumer Protection in the 21st Century, https://cdt.org/files/2018/08/CDT-FTC-comments-5-8-20-18.pdf

CONSUMERS RELINQUISHING THEIR RIGHTS TO THEIR PERSONAL DATA

While numerous federal agencies in the U.S. and across the globe develop privacy and security legislation that protects patient data, consumers continue to broadly share PHI on the internet. Of significant importance is the growing number of consumers who voluntarily give away their personal genomic data, without any restrictions, to the DNA market. Sequencing the first human genome took more than a decade and cost hundreds of millions of dollars. Now it takes less than 24 hours and can be done for less than $1,000.[v] This technological advance has led to more than 200 direct-to-consumers genealogy sites, with the collection of biological data being the true return on investment. The average consumer is not contemplating the ramifications of providing his or her DNA to a genealogy company, nor reading the FTC's guidance on Direct-to-Consumer Genetic Tests.

Most consumers share genomic data on these sites to answer questions about their *own* genealogy; however, online genomics companies see another market for the use of the data they collect. Use of DNA data for clinical research is a lucrative market. Several years ago, 23andMe was able to demonstrate potential usage of its DNA data by recruiting 450,000 members for a study on depression.[vi] As 23andMe's depression study and heavy investment in wearable technologies illustrate, more companies outside of the traditional healthcare arena are attempting to tackle problems such as addiction, mental health conditions, and chronic pain. A tremendous amount of data is required for research, and DNA databases from these corporations can fill a void.

> "Data is the new oil."
>
> *-Edward You, Weapons of Mass Destruction Biological Countermeasures Unit, FBI*

In July 2018, 23andMe announced that GlaxoSmithKline (GSK) invested $300 million in the company to gain exclusive access to 23andMe's genetic database of more than 5 million people.[vii] Pharmaceutical companies are able to custom-make drugs with DNA data and GSK intends to use 23andMe's database to develop an experimental Parkinson's drug. As more pharmaceutical companies begin to partner with genealogy groups, there are likely to be legal and ethical questions about the appropriate use of consumer data. Many initiatives are beginning to look at genomic security and safety in the U.S. and globally.

Initiatives Addressing Genomic Security

- **National Academy of Sciences.** With an initiative called *Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy while Sustaining Innovation and Growth,* an ad hoc committee of the National Academies of Sciences, Engineering, and Medicine will convene to consider strategies for safeguarding and sustaining the economic activity driven by research and innovation in the life sciences, collectively known as the bioeconomy.[viii]
- **National Institute of Health (NIH).** When the U.S. Congress approved $2 Billion to increase NIH Funding, the law included an amendment from Senator Marco Rubio (R-FL) that requires the

[v] https://www.genome.gov/sequencingcostsdata/
[vi] https://www.23andme.com/depression-bipolar/ AND https://www.nature.com/articles/ng.3623
[vii] https://www.healthcareitnews.com/news/23andme-lands-300-million-investment-glaxosmithkline
[viii] http://nas-sites.org/dels/studies/bioeconomy/

HHS Secretary to submit a report on the circumstances in which CMS may be providing payments to, or otherwise funding, entities that process genome or exome data in China or Russia.[ix]

- **The Committee on Foreign Investment in the United States (CFIUS).** CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the United States (covered transactions), to determine the effect of such transactions on the national security of the United States. On August 1, the Senate passed the Foreign Investment Risk Review Modernization Act (FIRRMA) as part of the 2019 defense authorization bill.[x]

Final Thoughts on Developing a Values Framework

Despite the shortcomings of HIPAA, it has survived more than two decades. A July 2018 article in the Journal of the American Medical Association (JAMA) by Glenn Cohen emphasized the surprising longevity of the original HIPAA framework. "HIPAA has accomplished its primary objective: making patients feel safe giving their physicians and other treating clinicians sensitive information while permitting reasonable information flows for treatment, operations, research, and public health purposes."[xi] Now, policymakers and industry leaders need to ensure that new privacy and security regulations have the ability to evolve with the explosion of new technologies.

New technologies have pushed society to reconsider current models for privacy and ethics and are raising important questions about individual liberty, dignity, and autonomy. Companies are facing enormous pressure to build and deploy ethical, privacy-protective, and inclusive products. The decisions made by developers and product managers, as they develop apps, are critical. The Center for Democracy & Technology and many other groups are beginning to explore a values framework for new technology. Recommendations focus on individual dignity, corporate stewardship, and social good.

> "Technology companies need a values framework, a HIPAA for fairness."
>
> *-Michelle DeMooy, Privacy and Data Specialist*

Given the rapid speed of technology development, it may be impossible for legislators to ensure federal and state policies address all consumer concerns. To make matters more complex, consumer concerns about the privacy of their data vary greatly. Before developing strict privacy policies, policymakers and industry leaders may want to first focus on developing a values framework to guide the future use of personal health information.

[ix] https://blog.ashg.org/2018/10/11/congress-approves-2b-nih/

[x] https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius and https://corpgov.law.harvard.edu/2018/08/26/the-cfius-reform-bill/

[xi] https://jamanetwork.com/journals/jama/fullarticle/2682916