The Evolving Regulatory and Commercial Environment for Digital Health and AI

Commercialization Considerations for Digital Health and AI

By Sharon Klein, Partner, kleins@pepperlaw.com and Karen Shin, Associate, shink@pepperlaw.com | Pepper Hamilton, LLP

Table of Contents

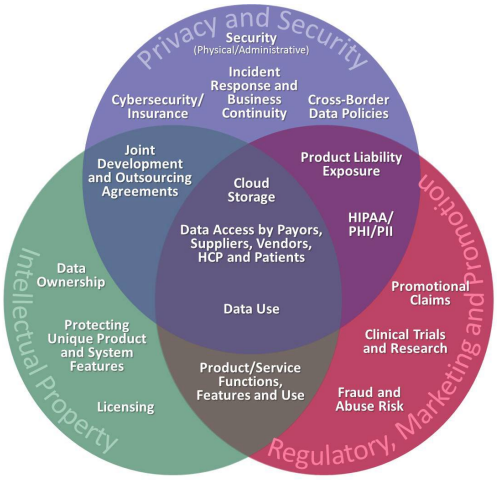
The Evolving Regulatory and Commercial Environment for Digital Health and AI

Commercialization Considerations for Digital Health and AI

By Sharon R. Klein, kleins@pepperlaw.com, and Karen Shin, shink@pepperlaw.com

Introduction

As developers and investors seek to commercialize software, medical devices, mobile medical applications and the data they generate, they must undertake a comprehensive legal analysis of various regulatory, commercial and intellectual property factors in order to weigh the risk profile against the reward they may achieve in the marketplace. In this article, we will consider a hypothetical developer that has created a mobile medical application to assist diabetics with controlling their health. The app displays current insulin levels from a glucometer, suggests a diet and exercise plan, and links to various educational resources. We will analyze this hypothetical in several parts: regulatory, HIPAA andprivacy and security, intellectual property and commercial considerations.



Regulatory Considerations

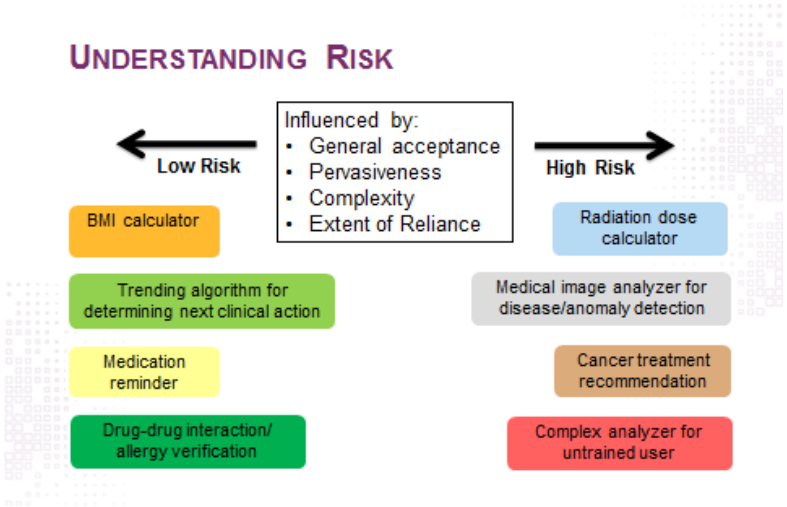
An important initial consideration is whether the hypothetical mobile medical app is regulated by the Food and Drug Administration (FDA) or the Federal Trade Commission (FTC). We will describe the various agencies' regulatory purviews, but first know that the FTC

has anticipated this question and has an interactive tool to help assess the scope of regulatory oversight and which regulators may be involved.[1]

FDA

This article will not attempt to delve into all aspects of FDA regulation but will focus on software as a medical device.

Software as a medical device (SaMD) is defined as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[2] The intention of the developer in creating the software application is key to how the FDA will categorize the SaMD based on the risk to patient safety, and thus will determine whether the FDA actively regulates the SaMD. The chart below demonstrates a risk analysis for SaMD.



On September 27, 2019, the FDA published six guidance documents clarifying the agency's interpretation of, and enforcement policies in light of, the 21st Century Cures Act (Cures Act).[3] These guidances largely follow the guidances that the FDA has issued for years on

[1] *See* FED. TRADE COMM'N, MOBILE HEALTH APPS INTERACTIVE TOOL (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[2] U.S. FOOD & DRUG ADMIN., SOFTWARE AS A MEDICAL DEVICE (SAMD) (2018), https://www.fda.gov/medical-devices/digital-health/software-medical-device-samd.

[3] U.S. FOOD & DRUG ADMIN., CLINICAL DECISION SUPPORT SOFTWARE DRAFT GUIDANCE (2019), https://www.fda.gov/media/109618/download; U.S. FOOD & DRUG ADMIN., CHANGES TO EXISTING MEDICAL SOFTWARE POLICIES RESULTING FROM SECTION 3060 OF THE 21ST CENTURY CURES ACT (2019), https://www.fda.gov/media/109622/download; U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS (2019), https://www.fda.gov/media/80958/download; U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES (2019), https://www.fda.gov/media/90652/download; U.S. FOOD & DRUG ADMIN., OFF-THE-SHELF SOFTWARE USE IN

SaMD. Below we discuss key takeaways from three relevant guidance documents: "Clinical Decision Support Software," "Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act," and "Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices."

1. Clinical Decision Support (CDS) Software

The CDS Software guidance is a revised draft guidance and distinguishes CDS that does and does not meet the definition of a device (Device CDS and Non-Device CDS, respectively) in the context of the Federal Food, Drug, and Cosmetic Act (FD&C Act)[4] section 520(o), as amended by the Cures Act.[5]

Section 3060(a) of the Cures Act amended FD&C Act section 520(o) by excluding certain software functions from the definition of "device."[6] As you will see, the intention behind the device's use and the fact that a health care professional (HCP) should not primarily rely on the data delivered by the device are key drivers in determining the classification. To be excluded from the device definition and be considered a Non-Device CDS, **all** four of the following criteria must be met:

- not intended to acquire, process or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system
- intended for the purpose of displaying, analyzing or printing medical information about a patient or other medical information
- intended for the purpose of supporting or providing recommendations to an HCP about prevention, diagnosis or treatment of a disease or condition
- intended for the purpose of enabling an HCP to independently review the basis for the recommendations that the software presents so that it is not the intent that the HCP rely

---

MEDICAL DEVICES (2019), https://www.fda.gov/media/71794/download; U.S. FOOD & DRUG ADMIN., MEDICAL DEVICE DATA SYSTEMS, MEDICAL IMAGE STORAGE DEVICES, AND MEDICAL IMAGE COMMUNICATIONS DEVICES (2019), https://www.fda.gov/media/88572/download.

[4] 21 U.S.C. § 301 *et seq.*

[5] U.S. FOOD & DRUG ADMIN., CLINICAL DECISION SUPPORT SOFTWARE DRAFT GUIDANCE (2019), https://www.fda.gov/media/109618/download.

[6] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 § 3060(a).

primarily on any of the recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.[7]

Some examples of Non-Device CDS include:

- software that provides recommendations to HCPs by matching patient-specific information (*e.g.*, diagnosis, treatments, allergies, signs or symptoms) to reference information the medical community routinely uses in clinical practice to facilitate assessments of specific patients, and provides an explanation that the basis of the recommendation is developed from authoritative medical sources with citations to those materials
- software that provides HCPs with recommendations on the use of a prescription drug that are consistent with FDA-required labeling and describes that the recommendations are based on the labeling so that the HCP does not primarily rely on the software's recommendation
- software that compares patient signs, symptoms or results with available practice guidelines (institutions-based or academic/clinical society-based) to recommend condition-specific diagnostic tests, investigations or therapy, and describes that the guidelines are the basis for the recommendation so that the HCP does not rely primarily on the software's recommendation.[8]

However, CDS software is considered a "device" if the intended user is a patient or caregiver and the software function is intended for the user to rely on the recommendations that the software presents.[9] If the CDS software is a Device CDS, then the FDA will apply a risk-based policy for regulation by leveraging the International Medical Device Regulatory Forum (IMDRF) framework, which categorizes the risk posed by an SaMD by (1) the significance of information provided by the SaMD (*i.e.*, whether the SaMD's function is to inform clinical management, drive clinical management, or treat or diagnose) and (2) the state of the health care situation or condition (*i.e.*, critical, serious or non-serious).[10]

The FDA plans to actively regulate Device CDS functions for:

---

[7] U.S. FOOD & DRUG ADMIN., *supra* note 5, at 6-7.

[8] *Id.* at 18-20.

[9] *Id.* at 8-9.

[10] *Id.* at 13.

- HCPs that are intended (using the IMDRF framework) to "inform clinical management" for "serious or critical situations or conditions," and that are not intended for the HCP to be able to independently evaluate the basis for the software's recommendations
- patients that are intended (using the IMDRF framework) to "inform clinical management" for a "non-serious situation or condition," and that are not intended for the patient to be able to independently evaluate the basis for the software's recommendations
- patients that are intended to "inform clinical management" for "a serious or critical situation or condition," whether or not the software is intended for the patient to be able to independently evaluate the basis for the software's recommendations.[11]

The FDA does *not* intend to actively regulate Device CDS for:

- HCPs that are intended (using the IMDRF framework) to "inform clinical management" for "non-serious situations or conditions"
- patients that are intended to "inform clinical management" for "non-serious situations or conditions," and that are intended for the patient to be able to independently evaluate the basis for the software's recommendations.[12]

2. Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act

In this final guidance document, the FDA details the changes to the existing guidance documents relating to the regulation of the software functions described in FD&C Act sections 520(o)(1)(A)-(D).[13]

The FDA states that it will not enforce the requirement imposed by the Cures Act exemption that certain electronic health records be certified by the Office of the National Coordinator for Health Information Technology.[14] The FDA also explains that the following types of software functions described by the Cures Act exemption for electronic health records do not meet the existing FD&C Act definition of "device" in any event:

- software function intendedfor administrative support of a health care facility

[11] *Id.* at 23-24.

[12] *Id.* at 20-21.

[13] U.S. FOOD & DRUG ADMIN., CHANGES TO EXISTING MEDICAL SOFTWARE POLICIES RESULTING FROM SECTION 3060 OF THE 21ST CENTURY CURES ACT (2019), https://www.fda.gov/media/109622/download.

[14] *Id.* at 8.

- software function intended for maintaining or encouraging a healthy lifestyle
- software function intended to serve as electronic patient records
- software function intended for transferring, storing, converting formats, and displaying data and results.[15]

The FDA will issue a separate guidance document to explain its approach to health IT systems that contain both non-device functions and device functions.[16]

3. Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices

In this updated final guidance on medical device data systems (MDDS), the FDA acknowledges the inconsistency between the definition of MDDS in 21 C.F.R. § 880.6310 and the definition of device in the FD&C Act, as amended by the Cures Act.[17] Under 21 C.F.R. § 880.6310, MDDS include both software and hardware, while the Cures Act exempts certain MDDS software functions from the definition of device.[18] The FDA clarifies that MDDS hardware are devices under the FD&C Act, but that it will continue to exercise enforcement discretion for these devices, as it has since 2015 when it published the guidance document "Policy for Device Software Functions and Mobile Medical Applications."[19]

The FDA further clarifies what constitutes a "Non-Device MDDS" and a "Device MDDS." A Non-Device MDDS is a software function that is *solely* intended to transfer, store, convert formats, or display medical device data or medical imaging data.[20] However, a Non-Device MDDS does not modify data or control the functions or parameters of any connected medical device.[21]

Additionally, software functions intended to generate alarms or alerts or prioritize patient-related information on multipatient displays, which are typically used for active patient

---

[15] *Id.* at 4-11.

[16] *Id.* at 8.

[17] U.S. FOOD & DRUG ADMIN., MEDICAL DEVICE DATA SYSTEMS, MEDICAL IMAGE STORAGE DEVICES, AND MEDICAL IMAGE COMMUNICATIONS DEVICES 2 (2019), https://www.fda.gov/media/88572/download.

[18] *Compare* 21 C.F.R. § 880.6310 *with* 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 § 3060(a).

[19] U.S. FOOD & DRUG ADMIN., *supra* note 17, at 2.

[20] *Id.*

[21] *Id.*

monitoring, are considered device software because these functions involve analysis or interpretation of laboratory tests or other device data and results.[22] Software functions that analyze or interpret medical device data in addition to transferring, storing, converting formats or displaying clinical laboratory test or other device data are also still considered devices and subject to the FDA's regulatory oversight, unless they meet the criteria in FD&C Act section 520(o)(1)(E).[23]

Consistent with the Cures Act, the FDA notes that, if a product contains both Non-Device MDDS and Device MDDS ("a multiple function device product"), the FDA does not intend to enforce the FD&C Act requirements for either part at this time.[24] However, the FDA will provide recommendations on the regulation of multiple function device products in a separate guidance document.[25]

Based on the FDA pronouncements, our hypothetical diabetes application's intended use to promote a healthy lifestyle provides a low risk to patient safety and will not be actively regulated by the FDA based on the FDA's "General Wellness: Policy for Low Risk Devices" final guidance.[26]

That guidance defines two categories of intended general wellness uses: (1) an intended use that relates to maintaining or encouraging a general state of health or a healthy activity or (2) an intended use that relates the role of a healthy lifestyle in helping to reduce the risk or impact of certain chronic diseases or conditions and where it is well understood and accepted that healthy lifestyle choices may play an important role in health outcomes for the disease or condition.[27]

The Regulatory Role of the FTC and Others

Even if not regulated by the FDA, the FTC and multiple states have privacy and security laws focusing on mobile medical applications and the internet of things. The FTC

---

[22] *Id.* at 3-4.

[23] *Id.* at 5.

[24] *Id.* at 6.

[25] *Id.*

[26] U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES (2019), https://www.fda.gov/media/90652/download.

[27] *Id.* at 3.

mandates privacy and security by design/default in its seminal guidance "Protecting Consumer Privacy in an Era of Rapid Change."[28]

It is true that you cannot have privacy without security. An analysis of an application's security posture will be essential to any commercial buyer as well as to the regulatory authorities. The FDA has issued numerous guidance documents focused on security of mobile medical apps (see below), and administrative, technical and physical security of protected health information is required for HIPAA compliance. Moreover, the FTC has issued multiple guidance documents on security, including "Protecting Consumer Privacy in an Era of Rapid Change"[29] and "Start with Security, a Guide for Business."[30] Many states have followed suit with examples including the California Internet of Things Act,[31] the California Attorney General's report "Privacy on the Go – Recommendations of the Mobile Ecosystem,"[32] and the Massachusetts Data Security Regulation to name a few.[33] Other guidance from the FTC includes:

- "Internet of Things – Privacy and Security in a Connected World"[34]
- "Self-Regulatory Principles for Online Behavioral Advertising"[35]
- "Mobile Privacy Disclosures: Building Trust Through Transparency," which promotes more effective mobile privacy disclosures[36]

---

[28] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[29] *Id.*

[30] FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[31] Cal. Civ. Code §§ 1798.91.04-1798.91.06.

[32] CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf?.

[33] 201 C.M.R. 17.00 *et seq.*

[34] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[35] FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[36] FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

- "App Developers: Start with Security," which provides recommendations to app developers for addressing mobile app security[37]
- "Marketing Your Mobile App: Get It Right from the Start," which gives guidelines to comply with truth-in-advertising standards and basic privacy principles[38]
- "What's the Deal?: An FTC Study on Mobile Shopping Apps," which provides guidelines addressed to developers of shopping apps.[39]

Also the Health Sector Coordinating Council (HSCC), a public-private partnership mandated by section 405(d) of the Cybersecurity Act of 2015 (Pub. L. 114-113), published "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" in December 2018.[40] It provides a common set of voluntary, consensus-based and industry-led guidelines, best practices, methodologies, procedures and processes to reduce cybersecurity risks. It consists of a comprehensive discussion of security in four volumes:

- "Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations," which discusses the 10 cybersecurity practices along with sub-practices for small health care organizations
- "Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations," which discusses the 10 cybersecurity practices along with sub-practices for medium and large health care organizations
- "Resources and Templates," which includes a variety of cybersecurity resources and templates for end users to reference
- "Cybersecurity Practices Assessments Toolkit (Appendix E-1)," a tool intended to help organizations prioritize their cyber threats and develop their own plans using the assessment methodology outlines in the "Resources and Templates" volume.

---

[37] FED. TRADE COMM'N, APP DEVELOPERS: START WITH SECURITY (May 2017), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security.

[38] FED. TRADE COMM'N, MARKETING YOUR MOBILE APP: GET IT RIGHT FROM THE START (2013), https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf.

[39] FED. TRADE COMM'N, WHAT'S THE DEAL?: AN FTC STUDY ON MOBILE SHOPPING APPS (2014), https://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf.

[40] U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTHCARE & PUB. HEALTH SECTOR COORDINATING COUNCILS, HEALTH INDUSTRY CYBERSECURITY PRACTICES: MANAGING THREATS AND PROTECTING PATIENTS (2018), https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.

The volumes highlight five cyber risks for the health care industry:

- email phishing attacks
- ransomware attacks
- loss or theft of equipment or data
- insider, accidental or intentional data loss
- attacks against connected medical devices that may affect patient safety.[41]

The HSCC also describes 10 cybersecurity threats:

- email protection systems
- endpoint protection systems
- access management
- data protection and loss prevention
- asset management
- network management
- vulnerability management
- incident response
- medical device security
- cybersecurity policies.[42]

Finally, the FDA has issued multiple guidances imposing security on mobile medical devices throughout the regulatory life cycle — pre- and post-market:

- "Postmarket Management of Cybersecurity in Medical Devices" (Dec. 28 2016), which encourages manufacturers to address cybersecurity throughout a product lifecycle and cautions about exploitation of networked devices[43]
- "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Oct. 18, 2018), a draft guidance that covers the FDA's recommended device

[41] *Id.* at 14.

[42] *Id.*

[43] U.S. FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (2016), https://www.fda.gov/media/95862/download.

design, labeling and documentation for premarket submissions for connected devices, building on 2013 and 2014 guidances[44]

- "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Oct. 2, 2014),[45] which covers the following topics:
  - information security requirements:
    - confidentiality
    - integrity
    - availability
  - security guidelines:
    - limited access
    - trusted content
    - fail-safe and recovery measures
  - emergency issues
  - documentation:
    - risk analysis
    - update control
    - disabling code
  - industry response:
    - existing devices
    - no retroactive implementation
    - transition period
    - intended use
- "Radio Frequency Wireless Technology in Medical Devices" (Aug. 14, 2013).[46]

In summary, any mobile medical device must demonstrate its security in transmission and storage of personal information in order to be a viable candidate for any commercial use.

---

[44] U.S. FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES DRAFT GUIDANCE (2018), https://www.fda.gov/media/119933/download.

[45] U.S. FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (2014), https://www.fda.gov/media/86174/download.

[46] U.S. FOOD & DRUG ADMIN., RADIO FREQUENCY WIRELESS TECHNOLOGY IN MEDICAL DEVICES (2013), https://www.fda.gov/media/71975/download.

Intellectual Property Considerations — Data Ownership and Use

In order for a developer to commercialize and obtain value for a device itslf and the content it generates, the developer must consider ownership rights in the device and the data. The developer cannot convey to a buyer what it does not own.

We will not consider here the software or hardware patents or other intellectual property of the device itself, but rather focus on data ownership and transfer of health data from the patients/consumers (end user data).

Who owns the data and whether that data can be conveyed is a complex matter. In most instances, conveying end user data will require express consent (most often pursuant to online terms of use or privacy policies), unless it can be demonstrated that the data transfer is related to treatment, payment or operations of a health care-covered entity, which is a safe harbor from consent under HIPAA (see below).

HIPAA Analysis

A. Background of Health Insurance Portability and Accountability Act (HIPAA)

The federal statutes and regulations that create the HIPAA regulatory scheme set out specific parameters for the use and disclosure of certain information relating to an individual's demographic data, health status, receipt of health care, and payment for health care, which is collected/used as part of a covered HIPAA relationship (collectively, protected health information or PHI).[47] If data meets the definition of PHI, it may only be used or disclosed as explicitly permitted or required by HIPAA.[48] When determining whether a particular use or disclosure is permitted, two questions are critical:

- What is the source of the data?

---

[47] PHI is data that (a) is transmitted or maintained by or in electronic media, or in any other form or medium, and (b) is "individually identifiable health information," which is "information that is a subset of health information, including demographic information collected from an individual, and:

> …
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual". 45 C.F.R. § 160.103.

[48] 45 C.F.R. § 164.502.

- What is the purpose of the use or disclosure?

With regard to the source of the data, an individual's medical and related information is only PHI if it is created or received by a covered entity, or a business associate acting on behalf of a covered entity.[49] If not, the data is not PHI and is not subject to HIPAA's limitations on uses and disclosures (although it will be subject to federal and state laws governing personal information).

If data is PHI, it may be used or disclosed (a) for the purposes of treatment, payment or health care operations without the necessity of patient authorization; (b) pursuant to and in compliance with a valid authorization executed by the individual to whom the information relates, or the individual's personal representative; or (c) for other specific purposes, such as public health monitoring, which are not relevant here.[50]

B. What Is the Source of the Data?

1. Data Obtained From the Patient/Consumer Is Not PHI.

In our hypothetical example, the end user diabetic is not a covered entity and is not acting on behalf of a covered entity or a business associate. Thus, the data that the patient transmits even to its HCP, such as the patient's name, contact information, prescription medications, treating provider, lifestyle and wellness information is not PHI, and is not subject to HIPAA.

2. Data Obtained From Organizations That Are Not Covered Entities or Business Associates Is Not PHI.

Consider whether some of the information in the hypothetical application may be obtained by the developer from pharmaceutical manufacturers of insulin and included in the mobile medical application. This data may include whether the patient is eligible for a co-pay assistance program and the patient's history of filling prescriptions for a particular medication. Whether or not this data is subject to HIPAA depends on its original source, and the purpose for which it was disclosed to the pharmaceutical manufacturer. If it was created or received by a covered entity or business associate, and disclosed to the pharmaceutical manufacturer for a HIPAA-permitted purpose, then the data is PHI subject to HIPAA and may only be used to send

[49] 45 C.F.R. § 160.103.

[50] *Id.*

patient messages for the same purpose as the original disclosure. If, however, the data was created by the pharmaceutical manufacturer or another entity not regulated by HIPAA, the data is not PHI and is subject only to any limitations agreed to when the information was collected and other applicable regulations, such as the FTC's consumer protection regulations.

3. Data Obtained By or on Behalf of a Covered Entity Is PHI.

Any health data identifiable to a patient that the developer obtains from a covered entity, such as the patient's provider, pharmacy or health plan, or a third-party business associate thereof, would be PHI.

C. What Is the Purpose of the Use or Disclosure?

Under HIPAA, "a covered entity or business associate may not use or disclose [PHI], except as permitted or required by" 45 C.F.R. Part 160, Subpart C, or 45 C.F.R. Part 164, Subpart E.[51] In our hypothetical, the developer is not a covered entity and does not have a business associate relationship with any covered entity. However, the developer does have a sub-contractor business associate relationship with certain business associates. In order for those business associates to disclose PHI to the developer, the purpose of the disclosures must (1) fall within the activities in which the business associate engages for the covered entity and (2) be set forth in a sub-contractor business associate agreement between the business associate and the developer. Further, in order for the developer to use the PHI in the application, this use must be consistent with (1) the purpose of the disclosure of the PHI by the covered entity to the business associate and (2) the purpose of the disclosure by the business associate to the developer.[52]

1. Disclosures for the Purposes of Treatment, Payment and Health Care Operations Are Generally Permissible.

A covered entity, or business associate acting on behalf of a covered entity, may use and/or disclose a patient's PHI for the purpose of treatment, payment or health care operations activities of the covered entity. Covered entities may be physicians, hospitals, pharmacies and health plans, which engage the business associates to assist with certain services.

---

[51] 45 C.F.R. § 164.502(a).

[52] In certain cases, a business associate, or a subcontractor business associate, may use or disclose PHI for the entity's "proper management and administration." 45 C.F.R. § 164.504(e)(2)(i)(A). In order for this use or disclosure to be permissible, the business associate agreements down the line must explicitly permit their occurrence.

"Payment," is defined as:

> (1) The activities undertaken by: (i) ... a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) [such] activities ... relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage...; (iii) Billing, claims management, collection activities,...; [and] (v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services....[53]

"Treatment" means:

> [T]he provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or by the referral of a patient for health care from one health care provider to another.[54]

"Health care operations" are certain administrative, financial, legal and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.[55] These activities, which are limited to the activities listed in the definition of "health care operations" at 45 C.F.R. 164.501, include:

- conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination
- reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing or credentialing activities
- underwriting and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to health care claims
- conducting or arranging for medical review, legal and auditing services, including fraud and abuse detection and compliance programs

[53] 45 C.F.R. § 164.501.

[54] *Id.*

[55] *Id.*

- business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity
- business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.[56]

2. Disclosures That Use PHI Obtained With a Valid HIPAA Authorization Are Permitted for Those Specific Purposes.

If the hypothetical developer is using PHI and there is no exception for treatment, payment or operations, then another avenue for end user consent may be to have a covered entity obtain an authorization under HIPAA. "Except as otherwise permitted or required …, a covered entity may not use or disclose [PHI] without an authorization that is valid under [45 C.F.R. § 164.508(a)(1).] When a covered entity obtains or receives a valid authorization for its use or disclosure of [PHI,] such use or disclosure must be consistent with such authorization."[57] Such an authorization must contain specific elements, including:

- a specific and meaningful description of the information to be used or disclosed
- the identification of the class of persons (need not be specific names, may be treating physician, insurer, etc.) authorized to make the requested use or disclosure
- identification of the developer as the entity to which the PHI may be disclosed, and which may further use the PHI to send messaging
- a description of each purpose of the requested use or disclosure
- an expiration date or an expiration event
- signature of the individual and date.

The authorization also must contain certain required statements and be written in plain language, and a copy of the executed authorization must be made available to the patient.[58]

---

[56] *Id.*

[57] 45 C.F.R. § 164.508(a)(1)

[58] 45 C.F.R. § 164.508(c).

Once these authorizations are obtained, the developer may use the PHI it obtains from the business associates for the purposes set forth in the authorization.

3. Disclosures for "Marketing" Purposes Require Patient Authorization.

Generally, uses and disclosures made for "marketing" purposes are prohibited unless the patient first signs an authorization permitting these activities.[59] And, "if the marketing involves financial remuneration, … to the covered entity from a third party, the authorization must state that such remuneration is involved."[60] HIPAA defines the term "marketing" as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."[61] There are, however, certain types of disclosures that are excepted from this definition. Specifically, "marketing" does not include (1) certain refill reminder communications that a covered entity or business associate is paid to make or (2) communications for treatment and health care operations purposes, as long as the covered entity is not paid to make such communications.[62]

4. Consent of End User

If the data collected by the hypothetical diabetes application does not constitute PHI under HIPAA transferred in accordance with treatment, payment or operations, and no HIPAA authorization is given, then another kind of consent is required. To evaluate consent, a developer should consider the touch points it has with the end user where a consent document can be most efficiently obtained. Generally, the best place for consent in a mobile medical application is in the terms of use or a privacy policy that must be clicked through to access the application. The consent must conform to the FTC's principles of consumer protection and applicable state law. Under section 5 of the FTC Act, consents must not be obtained in a false or misleading way.[63] An end user must be able to know why his or her data is collected, for what purposes and when it is shared. These principles are echoed in many state laws — California

---

[59] 45 C.F.R. § 164.508(a)(3).

[60] *Id.*

[61] 45 C.F.R. § 164.501.

[62] *Id.*

[63] *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

alone has dozens of privacy laws regulating consumer consent, especially in privacy policies and terms of use.[64]

California medical privacy law prohibits using personal medical information for direct marketing purposes without consent.[65] Additionally, California recently adopted a regulatory regime similar to Europe in the California Consumer Privacy Act (CCPA). The CCPA[66] creates the consumer rights to know and delete personal information collected by a business, opt out of the sale of personal information, and not be discriminated against for exercising any of the foregoing rights.[67] The CCPA also contains several notice provisions, requiring businesses to inform consumers (defined as California residents, which includes employees[68]) about their rights under the statute and the business's collection and disclosure practices at or before the collection of the consumer's personal information.[69] The CCPA provides for a qualified private right of action if a consumer's nonredacted or nonencrypted personal information is the subject of unauthorized access and exfiltration, theft or disclosure as a result of a business's violation of the duty to implement and maintain reasonable security procedures appropriate to the nature of the information.[70] After being hastily enacted in 2018 and after a series of amendments,[71] the CCPA went into effect on January 1, 2020. On October 10,

---

[64] *See* Cal. Civ. Code §§ 1798.83-1798.84 (California "Shine the Light" law); Cal. Civ. Code §§ 1798.91.04-1798.91.06 (California "Internet of Things" law); Cal. Bus. & Prof. Code §§ 22575-22579 (California Online Privacy Act); CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf?.

[65] Cal. Civ. Code § 1798.91.

[66] Sharon Klein et al., *California Consumer Privacy Act: European Style Privacy with a Twist*, PEPPER HAMILTON LLP (July 10, 2018), https://www.pepperlaw.com/publications/california-consumer-privacy-act-european-style-privacy-with-a-california-enforcement-twist-2018-07-10/.

[67] Cal. Civ. Code § 1798.100 *et seq.*

[68] Sharon Klein et al., *Deadline Looms for Employers to Provide CCPA Notices*, PEPPER HAMILTON LLP (Oct. 28, 2019), https://www.pepperlaw.com/publications/deadline-looms-for-employers-to-provide-ccpa-notices-2019-10-28/.

[69] Cal. Civ. Code § 1798.100.

[70] *Id.* § 1798.150.

[71] Sharon Klein et al., *Latest California Consumer Privacy Act Amendments Impact Business Compliance Initiatives*, PEPPER HAMILTON LLP (Sept. 16, 2019), https://www.pepperlaw.com/publications/latest-california-consumer-privacy-act-amendments-impact-business-compliance-initiatives-2019-09-16/.

2019, the California Attorney General released proposed regulations[72] implementing the statute.[73] The regulations for the CCPA will be finalized on July 1, 2020, which is when the Attorney General will begin its enforcement.[74]

These statutes mainly call for the consent documents, such as the terms of use and privacy policies, to spell out clearly and concisely what the application is collecting/sharing so that the end user has an informed choice and can consent before or at the time of collection. The issue the developer of our hypothetical diabetes application may have is that the developer has no direct touch point to obtain the consent of the patient end user. Consider that the physician may be registering for the mobile application and then allowing her patients access to the application. In such cases, the developer must contractually obtain assurances from the physician, or whoever is registering for the mobile application, that the physician has obtained the proper authorizations and consents from the end user. In the commercial transaction, the buyer of the mobile medical application company will require a representation and warranty to guarantee the contractual chain granting permission from the end user to consent to allow collection and use of the diabetes information collected by the application.

D. De-Identification and Databases

Let's say our hypothetical developer has not obtained end user consent but intends to rely on de-identification to compile data into a database that then can be remarketed and resold.

Compiling de-identified data into databases that can be commercialized is becoming challenging.

What is the standard for de-identification? Under HIPAA, there are two ways to de-identify data:

- elimination of 18 identifiers: names; all geographic subdivisions smaller than a state (including street address, city, county, precinct, ZIP code, and their equivalent genocodes); all elements for dates (except year) for dates that are directly related to an

[72] Sharon Klein et al., *California AG Releases Proposed CCPA Implementing Regulations*, PEPPER HAMILTON LLP (Oct. 11, 2019), https://www.pepperlaw.com/publications/california-ag-releases-proposed-ccpa-implementing-regulations-2019-10-11/.

[73] Cal. Dep't of Justice, California Consumer Privacy Act Regulations Proposed Text of Regulations (Oct. 10, 2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

[74] Cal. Civ. Code § 1798.185

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); telephone numbers; fax numbers; email addresses; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers (including license plate numbers); device identifiers and serial numbers; URLs; IP addresses; biometric identifiers (including finger and voice prints); full-face photographs and any comparable images; and any other unique identifying number, characteristic or code

- obtaining an expert opinion (usually from a statistician) that the data is property de-identified under the National Institute of Standards and Technology.[75]

Once de-identified, the regulations require that the data not be re-identified back to an unique individual. The smarter technology becomes, the harder it is to ensure that there is no re-identification.

Recently, Google has been at the center of privacy concerns due to its health-sharing collaborations with the University of Chicago Medical Center (the Medical Center) and Ascension, and is currently facing a class action and a federal inquiry related to HIPAA.

1. Google and the University of Chicago Medical Center

In May 2017, Google announced its partnership with the Medical Center to "research ways to use machine learning to predict medical events."[76] A few months later, the Medical Center transferred electronic health records (EHRs) of hundreds of thousands of individuals who were patients at the Medical Center from 2009 to 2016.[77] In its Notice of Privacy Practices and Admission and Outpatient Agreement and Authorization (Notice), the Medical Center promised patients that it would not disclose patient records to third parties for commercial purposes and would comply with federal and state privacy laws, including HIPAA,

[75] 45 C.F.R. § 164.514(b).

[76] Lisa Schencker, *U. of C. Medicine, Google Hope to Use Patterns in Patient Records to Predict Health*, CHI. TRIB., May 17, 2017, https://www.chicagotribune.com/business/ct-google-university-chicago-partnership-0518-biz-20170517-story.html.

[77] Daisuke Wakabayashi, *Google and the University of Chicago Are Sued Over Data Sharing*, N.Y. TIMES, June 26, 2019, https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html.

to protect and maintain the privacy and confidentiality of the records.[78] The Notice did not disclose that the Medical Center would transfer patients' medical records to Google or similar vendors, and did not give the Medical Center permission to disclose the records to entities like Google for any purpose whatsoever.[79]

In an article describing their research findings and the methodology employed in analyzing patients' medical records, Google and the Medical Center revealed that, while the EHRs were supposedly "de-identified," the date stamps and free-text medical notes from the records were maintained.[80] Patient demographics, provider orders, diagnoses, procedures, medications, laboratory values, vital signs and flowsheet data on both inpatients and outpatients were also included in these records.[81]

On June 26, 2019, a putative class action was filed in the federal court for the Northern District of Illinois by Dinerstein against Google and the Medical Center for the Medical Center's disclosure of EHRs to Google.[82] The complaint alleged that the date stamps and free-text notes that were maintained from the records immediately placed the transfer of the records outside of HIPAA's safe harbor provision, and that the Medical Center did not perform an expert determination before transferring the medical records to Google or alternatively, if it did hire an expert, did not make a finding that the risk of re-identification was small.[83] With the vast amount of personal information Google possesses and its powerful analytics capabilities, including Google's abilities to identify individuals' exact locations and time spent at a location, the complaint alleges that Google is easily able to re-identify the medical records it received from the Medical Center, with the help of the date stamps for admission and discharge and the free-text notes, which are not to be included in de-identified medical records.[84]

---

[78] Complaint at 20, *Dinerstein v. Google*, No. 1:19-cv-04311 (N. D. Ill. June 26, 2019).

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.* at 1.

[83] *Id.* at 21-22.

[84] *Id.* at 28.

The complaint further alleges that Google's receipt of the Medical Center's patient records was part of Google's longtime scheme to gain a foothold in the predictive health analytics industry:

- In 2008, Google attempted to gather consumer medical data by developing a service that allowed consumers to organize and store their personal health data and medical records on Google's platform, but this service was discontinued for a lack of consumer participation.
- In 2014, Google acquired a small startup named DeepMind that focused on bringing artificial intelligence and advanced machine learning to, among others, the health care industry.
- In 2015, Google and DeepMind participated in a study that processed patient data from the Royal Free NHS Foundation Trust (NHS). However, the Information Commissioner's Office, a UK data protection watchdog, announced that Google and DeepMind's agreement with NHS failed to comply with data protection law. Google and DeepMind responded by promising to protect patient privacy and announced that DeepMind would continue to operate independently and outside the reach of Google, and that Google would not have direct access to patient records. However, Google and DeepMind did not change any of their privacy practices, and in 2018 Google announced that it would fully absorb and take control of DeepMind Health, separating it from DeepMind and allowing Google to have access to health data collected and processed by DeepMind.[85]

The complaint also alleges that Google planned to gather consumer medical data to create its own EHR system and commercialize the Medical Center's medical records prior to obtaining them, as evidenced by the patent application it submitted in 2017.[86] The EHR system includes a computer memory storing de-identified EHR, a computer executing deep learning on those records in a standardized data structure format, and an interface for clinicians displaying the patient's past and predicted future clinical events.[87]

[85] *Id.* at 14-16.

[86] *Id.* at 17.

[87] *Id.*

Google and the Medical Center have already made several attempts to dismiss the class action, and have most recently alleged that the plaintiffs' attorney has a conflict of interest as an investor in a competing analytics company.[88] The lawsuit is still pending.

2. Google and Ascension

Similar to Google's partnership with the Medical Center, Google announced on November 11, 2019 that it had partnered with Ascension Health, a Catholic nonprofit health system operating in 21 states with 2,600 hospitals, clinics and other medical outlets.[89] Named Project Nightingale, Google would (1) build a search tool for medical professionals that would use machine-learning algorithms to process data and make suggestions about prescriptions, diagnoses and even which doctors to assign to, or remove from, a patient's team; (2) integrate Ascension's different areas of health data in the cloud; and (3) allow Ascension to use G Suite productivity tools to enable Ascension employees to communicate and collaborate with operations teams across Ascension sites of care.[90]

However, through this partnership, Ascension, without notifying patients or doctors, began sharing with Google the personally identifiable information of more than 50 million patients, such as names, dates of birth, lab tests, doctor diagnoses, hospitalization history, prescriptions and some billing claims and other clinical records.[91]

Google's public announcement of the partnership emphasized privacy and security, stating that Google adheres to industrywide regulations, including HIPAA, and has a business associate agreement with Ascension, which restricts the use of Ascension's data solely for providing services under the agreement and prohibits the combination of that information with Google consumer data.[92]

---

[88] Daniel R. Stoller, *U of Chicago Seeks Health Suit End on Alleged Attorney Conflict*, BLOOMBERG LAW, Nov. 14, 2019, https://news.bloomberglaw.com/privacy-and-data-security/u-of-chicago-seeks-health-suit-end-on-alleged-attorney-conflict.

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

[90] *Id.*

[91] Rob Copeland, *Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans*, WALL ST. J., Nov. 11, 2019, https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

[92] Shaukat, *supra* note 89.

On November 12, 2019, Department of Health and Human Services (HHS) Office of Civil Rights (OCR) Office Director Roger Severino announced that HHS OCR would inquire into the partnership and investigate whether HIPAA was violated.[93] In response, Google released an FAQ, stating that it ensures the privacy and security of patient data with technical and administrative safeguards and promising that the data would not be used to sell advertisements.[94] It further stated that a "limited number of Google employees have been approved by Ascension to potentially handle PHI in order to provide the services to Ascension."[95] However, at least 150 employees in different divisions of Alphabet Inc. (Google's parent company), including Google Brain (Google's artificial intelligence research team), had access to the patient data.[96] Moreover, it is unclear whether Google will combine its data with Ascension's to augment its services to Ascension (*e.g.*, predictive analytics based on both clinical and social data), which would be permissible under HIPAA.

Google's health data partnerships with the Medical Center and Ascension demonstrate how the health care industry is confronted with the "Goldilocks Dilemma," a phrase coined by Deven McGraw, the former Deputy Director of Health Information Privacy at HHS OCR and currently the general counsel and chief regulatory officer for consumer health technology startup Citizen. The Health Data Goldilocks Dilemma describes how to achieve the balance for "broader data interoperability and data sharing," with "enhanced data privacy and protection."[97] While sharing health information is essential for clinical care, powering medical discovery, and enabling health system transformation, the public is expressing greater concerns over the privacy of personal health data as large technology companies, like Google, break into the health care industry. The medical and personal data accumulated by technology companies using smart technologies, like Google, will need to be completely separated to protect the privacy of health data. HIPAA will also need to be updated to keep up with the technological

---

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

[94] Shaukat, *supra* note 89.

[95] *Id.*

[96] Copeland, *supra* note 91.

[97] Zoya Khan, *Announcing a New Series: "The Health Data Goldilocks Dilemma: Sharing? Privacy? Both?*, HEALTH CARE BLOG, July 22, 2019, https://thehealthcareblog.com/blog/2019/07/22/announcing-a-new-series-the-health-data-goldilocks-dilemma-sharing-privacy-both/.

advancements in health care — something Timothy Noonan, HHS OCR's Deputy Director for Health Information Privacy, says HHS OCR will focus on in 2020.[98]

Commercial Considerations

Once our hypothetical developer passes the regulatory hurdles for its mobile medical application and feels confident that it owns the data collected by the application, the developer may want to sell the small company formed to house the application.

Potential buyers want to be certain that the privacy/security of the application has passed regulatory and technical security. Common due diligence questions are illustrated below. The goal of diligence is to provide a compliance review to mitigate the liability to the potential buyer and to support the valuation desired by the seller. The diligence not only focuses on the practices of the seller but also those of its third-party vendors and suppliers with whom the personal data of individuals was shared. Security assessments of the seller and its third parties' practices may be required. A potential seller would be well-advised to have an external consultant or legal adviser assist with a compliance audit and security assessment relative to the technology and the data collection.

One important consideration is whether the developer is selling the mobile medical application tool itself plus the data derived from the prior use of the tool, whether in identified or de-identified form. Additional hurdles will be added if the data previously gathered from diabetics is included as part of the commercial valuation. If data is included, whether de-identified or identifiable, it is important that the end user consent allow transfer of the diabetes information of the user in the context of any merger/acquisition or other commercial transaction. The terms of use or privacy policies under which end user consent was obtained must be thoroughly analyzed. For example, the diabetic using the mobile application may have consented to use of her data only for research not commercialization.

A. Sample Due Diligence Questions

1. IT/Privacy/Security Diligence

The potential buyer will need a mini data map of the kinds of personal data collected, how it was used and with whom it was shared. This is important because the potential buyer

[98] Ayanna Alexander, *Patient Data, Cyber Threats, Surprise Billing Top OCR To-Do List*, BLOOMBERG LAW, Oct. 3, 2019, https://news.bloomberglaw.com/privacy-and-data-security/google-university-of-chicago-face-revamped-health-privacy-suit.

will be taking on the obligations of the seller under all applicable privacy laws, including HIPAA.

1.1. Please identify all types of personal information collected, used or processed by the company and the source of such information (*e.g.*, sourced from employees, customers, prospective customers, vendor personnel, third-party list providers, the internet). Examples of "personal information" include name; address; phone number; email address; persistent device identifiers (such as on mobile phones, tablets); government-issued identifiers, such as Social Security numbers, tax IDs, passport or driver's license numbers; financial account data (including payment card data); credit report or other consumer scoring data; medical or health care information; biometric data; geo-location data of individuals or devices (*e.g.*, collected from mobile devices); online or mobile tracking or monitoring data (*e.g.*, behavioral data collected through cookies or other web-tracking technologies); and sensitive demographic data (*e.g.*, age, race, ethnicity, sexual orientation). For all personal information, please identify:

i. the location of individuals from which such personal information is collected (*e.g.*, United States, European Union, Canada) and/or the source from which the personal information is received;

ii. the location (geographic, system and vendor, if applicable) where the personal information is stored;

iii. the identity of all third parties with whom personal information is shared, sold or licensed; and

iv. how the personal information is used/the business purpose for the collection, use or processing of such personal information.

Understanding what kind of PHI was collected, how it was acquired or transferred, and how it is used are key in ensuring the seller's compliance with HIPAA (*e.g.*, whether the seller's uses are aligned with HIPAA's permitted uses) and other applicable privacy laws.

1.2. Describe all sources and uses of protected health information, and means of acquisition or transmission thereof.

Proper privacy and security policies and procedures are critical in documenting the seller's compliance with HIPAA, including whether the seller has administrative, physical and technical safeguards in place. A potential buyer may ask for policies and policies from the preceding five years to ensure that the policies were actually followed in practice.

1.3. Please provide all written privacy policies and disclosures related to the privacy of employees, customers, consumers, patients and other individuals, including all policies governing privacy rights and expectations of employees and other persons working with the company (*e.g.*, independent contractors, temporary employees) and all disclosures to customers, consumers and third parties of the company's privacy practices, regardless of the medium in which such disclosures are made. "Privacy policies" include documents addressing the company's approach to collecting, using, sharing, transferring and/or disposing of personal information in any media. Examples include but are not limited to:

(i) internal policies and handbooks governing employee privacy duties and expectations;

(ii) list of HIPAA privacy and security officers;

(iii) website privacy statements and other public consumer privacy notices;

(iv) computer, internet and other systems' acceptable use policies;

(v) mobile device and laptop use policies;

(vi) clean desk/clear screen policies;

(vii) data classification policies;

(viii) policies and procedures relating to the de-identification and/or anonymization of personal information; and

(ix) record maintenance and retention policies.

To the extent that the company prepares any such policies and disclosures for its customers, please provide templates or samples of such policies.

1.4. Please provide a copy of each policy relating to information security within the company (*i.e.*, policies that address protection of the confidentiality, integrity and availability of the company's data, including personal data) and protection of all administrative, physical and electronic systems and facilities used in connection with the collection, use, storage, transfer, retention and disposal of company information, including personal data. To the extent that the company prepares any such policies for its customers, please provide templates or samples of such policies.

1.5. Please provide copies of all HIPAA, HITECH and data privacy and security compliance plans, notices, policies and procedures, including notification and reporting policies and data governance. Please describe what administrative, physical and technology safeguards are in place to protect the integrity of protected health information. To the extent that the company prepares any such compliance plans, notices, policies and procedures for its customers, please provide templates or samples of such policies. Please identify the person responsible for HIPAA and privacy and security compliance.

While the seller's privacy and security policies and procedures are essential for HIPAA compliance, most buyers also will require audit reports and assessments to determine the effectiveness of the seller's policies and procedures and data security practices. The reports and assessments reveal any potential risks and vulnerabilities to the confidentiality and integrity of personal data, and whether the seller has done anything to remediate these risks to the business.

1.6. Please provide copies of the company's data security control or regulatory audit reports for the last two years and identify any issues identified therein that have not been remediated.

1.7. Please provide copies of all HIPAA risk assessments or gap analyses performed.

1.8. Please provide a copy of any privacy compliance risk assessments, compliance audits, compliance certifications, whether conducted internally or by third parties (*e.g.*, HITRUST certification documents, SOC 2 Level 2 audit reports), privacy impact assessments and/or privacy-related data mapping the organization has undertaken in the last three years, and identify any exceptions, deficiencies or other issues identified therein that have not been fully remediated. Also provide a copy of the organization's scheme or method for classifying the sensitivity of data (*e.g.*, public, internal, confidential, restricted).

Questions relating to the proper de-identification of data collected will be judged using the NIST SP 800-53 standards. The potential buyer will want to know the methods of de-identification and how the de-identified data is shared and used to determine whether the seller is compliant with HIPAA's de-identification methods and whether there is a risk of re-identification.

1.9. Please identify all instances in which the company creates, uses, shares or otherwise processes anonymized and/or de-identified data based in whole or in part on personal information. For each instance, please describe the business purpose for which such anonymized and/or de-identified data is used.

1.10. Describe whether/how the company uses de-identified health information and describe the processes and standards utilized by the company for de-identifying such information.

1.11. Does the company commercialize, monetize, anonymize/de-identify or otherwise use personal information other than in connection with services provided to customers under written contracts?

Direct marketing is an area heavily regulated by federal and state agencies. A potential buyer will have specific questions about marketing authorizations and activities.

1.12. Describe uses of personal information made by the company or its agents in any direct marketing activities. "Direct marketing" includes commercial communications to individuals through direct hard copy mail, email, text messaging, faxes, telephone (including mobile phones) or other telemarketing means. To the extent known, please include the national residences of individuals who receive direct marketing from the company.

Where data is stored is important in understanding what federal, state or international laws that regulate personal data apply (*e.g.*, the GDPR). To determine whether international laws apply, a potential buyer will ask whether any of the seller's data is stored outside the United States. A potential buyer will also want to ensure that the seller is compliant with these laws and ask for documentation of compliance, including the seller's policies for cross-border transfers of personal data and for responding to data subject requests.

1.13. Does the company store any of its data related to the business, whether related to customers, employees, customers' patients or insureds, or otherwise, on servers located outside the United States?

1.14. To the extent not included in company privacy policies, please provide copies of any compliance policies (or describe unwritten policies), procedures or contract documents (*e.g.*, data transfer agreements) designed to assure the lawful transfer of personal data between the company and its affiliates or third parties, where such transfers either transmit or permit access to personal data across different national boundaries.

1.15. To the extent not included in company privacy policies, please describe any efforts the company has undertaken to analyze, plan for, and comply with legal requirements under Regulation (EU) 2016/679 (GDPR) or any applicable state laws regarding an individual's access to data, including any requirements to respond to requests from individuals for access to, deletion of, or other accounting of data and data practices.

A potential buyer will request information regarding any history of security breaches as well as any related notices provided and responses received. Information regarding any security breach is important because it will identify any past or pending litigation, complaints, administrative fines or penalties, and whether appropriate corrective action was taken.

1.16. Please identify whether the company ever has experienced an unauthorized intrusion into or penetration of its information technology/computer network system or otherwise experienced a breach of data security with respect to data stored on any of the company's servers or other media. If so, please provide the following information:

i. Describe the nature of the security breach, including the manner in which the breach was committed, the number of consumers/persons/customers affected, and the type and amount of data stolen, copied or intercepted;

ii. Provide all documents relating to the security breach, including internal assessments, letters to affected parties, pleadings filed in any resulting litigation or administrative complaint, and communications with law enforcement authorities; and

iii. Identify all remedial measures taken as a result of the security breach to prevent similar breaches in the future.

A potential buyer will also ask for information regarding any complaints received regarding the privacy and security of data and any self-disclosures or internal audit results relating to fraud and abuse to further identify whether the seller has any ongoing liability.

1.17. Please describe any complaints received by the company relating to the privacy or security of its data, and provide all documents relating to such complaints and any resulting investigations, mitigation, resolution strategies or remedial measures adopted.

1.18. Please provide copies of any self-disclosures to any governmental authorities, or internal audit results relating to fraud and abuse.

A potential buyer will inquire into whether the seller has experienced any IT system failures and whether any remediation steps were taken to ensure that the potential buyer can rely on the service in the ordinary course of its business.

1.19. Please describe any IT system failures in the last five years that have caused a disruption to the company's business, including any applicable remediation steps taken.

Insurance is critical in reducing the financial risks that may be incurred by a data breach and other security incidents, and a potential buyer will want to know whether the coverage is adequate in both scope and coverage limits. A potential buyer will want to know what is covered and how these coverages fit into the seller's risk profile.

1.20. Please provide copies of all insurance coverage (including primary and excess layers) for first and third-party losses related to or arising from cybersecurity incidents (including losses arising from data breaches), and other loss, corruption or unavailability of data, and claims of invasion of privacy or violation of privacy rights.

Agreements with third parties with whom personal data is shared are important in ensuring the privacy and confidentiality of personal data. This includes understanding the third party's access to the seller's personal data, whether the third party's data security practices are sufficient, and whether the agreements regarding indemnification, insurance, etc. are adequate. The seller's agreements with third parties are also important to understand whether the seller has any obligations to consumers and other third parties.

1.21. With regard to all third parties identified in response to Section 1.1(iii) above, provide all agreements or other authorizations related to the sharing of the personal information.

1.22. Identify all third parties to whom the company has granted access to the company's data used in the business for any purpose, and provide all agreements with such third parties.

A potential buyer will ask for all of the seller's business associate agreements to determine whether these agreements are compliant with HIPAA's requirements. Additionally, the potential buyer will inquire into how the seller assures its subcontractors or vendors are HIPAA compliant if there is no business associate agreement in place.

1.23. Does the company enter into business associate agreements with subcontractors that have access to protected health information maintained by the company; if not, how does the company assure/maintain downstream HIPAA compliance?

1.24. Please provide a copy of the company's form(s) business associate agreement and provide a schedule of all business associate agreements entered into by the company.

A potential buyer will ask for all agreements relating to the IT equipment, systems, software and services the seller uses to ensure that the seller has the proper intellectual property rights to them.

1.25. Please provide all agreements regarding the purchase or use of software, research, data or data services or computer or data processing equipment.

1.26. Please provide copies of all agreements relating to the provision of IT, data or internet-related products or services to or by the company, including, without limitation, outsourcing, internet service provider, maintenance and support, hosting, source code escrow and disaster recovery agreements, material software licenses and any other material agreements or arrangements relating to the company's use or possession of IT systems and services.

1.27. Please provide a description of and copies of documents relating to whether the company has access, or rights of access, to the source code of material licensed software in order to ensure adequate maintenance and updating of that software.

ATTACHMENT A

GUIDANCES WITH DIGITAL HEALTH CONTENT

https://www.fda.gov/medical-devices/digital-health/guidances-digital-health-content