Privacy as a competitive differentiator:

Building an effective and strategic healthcare privacy program

By Jiayan Chen, Partner, McDermott Will & Emery; Ryan Higgins, Partner, McDermott Will & Emery; Ty Kayam, Digital Health Attorney, Microsoft Corporation; Michael Hamilton, Chief Privacy Officer, Invitae Corporation

Contents

Privacy as a competitive differentiator:

Building an effective and strategic healthcare privacy program

By Jiayan Chen, Partner, McDermott Will & Emery; Ryan Higgins, Partner, McDermott Will & Emery; Ty Kayam, Digital Health Attorney, Microsoft Corporation; Michael Hamilton, Chief Privacy Officer, Invitae Corporation

The views, thoughts, and opinions expressed in this whitepaper belong solely to the authors and do not reflect the official policy or position of their respective organizations or any other organization with which the authors are affiliated.

I. Introduction

Privacy in the modern age of technology is not limited to a set of rules that restrict or prohibit how data can be used. Rather, it is a tool for empowering individuals as they navigate increasingly sophisticated and complex systems, and for enabling innovation and growth while protecting a basic individual right. This paper provides a comprehensive framework for building and managing a healthcare privacy program (also referred to throughout this paper as a healthcare privacy function) based on the collective insights from in-house and external privacy counsel. While this paper is not designed to comprise a generally applicable "gold standard" for a privacy program, we hope it can provide a practical framework that can be leveraged by privacy professionals in building and managing their particular healthcare privacy functions.

The importance of privacy laws to the healthcare industry and adjacent companies is growing for two primary reasons. [1]First, data has become an integral part of the business of healthcare, rather than an incidental byproduct of healthcare delivery. The volume of healthcare data being generated is growing exponentially, as is the power and sophistication of technologies that can analyze and derive insights from such data, such as artificial intelligence and machine learning algorithms. Healthcare organizations have increasingly come to view the collection and deployment of data as a core part of their business and growth.

While opportunities to leverage data proliferate, the legal climate as well as norms around data sharing and what constitutes meaningful privacy are evolving and becoming more complex. These dynamics are particularly evident in the healthcare industry as healthcare becomes increasingly consumer-oriented and powered by applications, platforms and devices that enable more continuous and comprehensive monitoring of and engagement with patients and consumers.

These trends make privacy compliance both more important and more complex. The complexity can make it harder for companies to achieve compliance with privacy laws and realize the underlying aims of privacy laws: to give individuals more visibility and control over their data. This paper is designed as a resource for privacy professionals that unpacks the practical components of a

healthcare privacy function and highlights the considerations for approaching privacy as a competitive differentiator rather than as merely a cost center.

In this paper, we first provide an overview of the privacy and related laws that may apply to a healthcare privacy function. We assume for this section the healthcare entity will be based in the U.S. but will be operating on a global scale.

Next, we distill the myriad requirements from these laws into eight core pillars. By pillars, we refer to a foundational category of work performed by a privacy function. Within each pillar, we then describe a set of specific activities that comprise that pillar. We also provide strategic and practical considerations for each pillar. While privacy functions will be as varied as the organizations they serve, from a team of one person working on privacy part-time to a privacy organization with scores of individuals, we believe these core pillars can be a framework for any healthcare organization's privacy function.

With these pillars as grounding, we then provide a set of recommendations for operating a healthcare privacy function that supports privacy compliance while also helping drive innovation and growth.

II. Overview of privacy legal landscape

Underlying any comprehensive privacy function within an organization is a patchwork of laws, rules, regulations and industry standards that set forth requirements for the confidentiality of protected health information, personal information and other categories of regulated information. These requirements — which focus on how certain information may be collected, maintained, used and disclosed — vary in terms of the entities they regulate, the kinds of information they regulate, the activities they regulate, and the extent and nature of restrictions and obligations they impose. Privacy laws also intersect with laws that regulate data security, for without safeguards in place for maintaining the security of regulated information, organizations would find it challenging to meaningfully uphold their obligations to protect data subjects' privacy and the confidentiality of their personal information.

This section provides an overview of various key federal, state and international laws that relate to data privacy, as well as industry standards that should be considered in the context of reviewing the overall set of requirements an organization may need to contend as it builds a privacy function. Not all these requirements will be applicable to each organization. However, it is helpful to understand the broader universe of key legal and regulatory requirements as an organization considers what obligations it may have, and as it does business or otherwise interacts with third parties that may be subject to different, or more extensive, privacy requirements.

A. Healthcare-specific laws

1. HIPAA

The Health Insurance Portability and Accountability Act,[2] the Health Information Technology for Economic and Clinical Health Act[3] and their implementing regulations, as amended,[4] comprise the key federal legal framework for health information privacy,[5] security[6] and breach notification[7] in the United States. The requirements of HIPAA apply to "covered entities" and "business associates" with respect to "protected health information."

"Protected health information" is a subset of health information that (1) is created or received by a healthcare provider, health plan or healthcare clearinghouse, (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual, and (3) identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[8] Not all health-related information is PHI. Health data that is generated through direct-to-consumer health or wellness services or solutions, such as health applications and fitness trackers, will generally fall outside the scope of HIPAA.

A "covered entity" is a (1) health plan, (2) healthcare clearinghouse, or (3) a healthcare provider that engages in certain electronic transactions as described by HIPAA involving PHI, including submitting electronic claims to third party payors ("standard transactions").[9] A "business associate" is a person that provides services to, or performs a function on behalf of, a covered entity involving the creation, receipt, maintenance or transmission of PHI by that person.[10]

HIPAA requires covered entities and business associates, among other things: (1) designate a privacy officer[11] and a security officer;[12] (2) maintain written privacy,[13] security[14] and breach notification[15] policies and procedures implementing HIPAA's privacy, security and breach notification standards; (3) as to covered entities, provide a "Notice of Privacy Practices" to individuals;[16] (4) perform an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the "Electronic PHI"[17] created, received, maintained and transmitted by the covered entity or business associate ("Security Risk Analysis");[18] (5) report "breaches"[19] of "unsecured PHI"[20] to affected individuals,[21] the secretary of the U.S. Department of Health and Human Services Office for Civil Rights,[22] and, under certain circumstances, the media;[23] (6) enter into "business associate contracts" where required;[24] and (7) train applicable "workforce" members regarding compliance with HIPAA.[25]

Not all health-related information is PHI. Health data that is generated through direct-to-consumer health or wellness services or solutions, such as health applications and fitness trackers, will generally fall outside the scope of HIPAA.

While both covered entities and business associates have obligations under HIPAA, the requirements for each entity differ. For instance, the HIPAA Privacy Rule regulates covered entities but does not directly apply to a business associate unless a covered entity delegates a function within the Privacy Rule to a business associate, in which case the business associate must comply with the requirements of the Privacy Rule in the performance of that delegated function. On the other hand, the HIPAA Security Rule applies to both covered entities and business associates, as does the Breach Notification Rule in relevant part. As discussed in Section III, these differences mean an organization's approach to HIPAA compliance and the structure of the healthcare privacy function should differ based on whether the organization is a covered entity, business associate, or both.

The OCR has authority to impose civil money penalties against covered entities and business associates for failure to comply with HIPAA's requirements. Penalties may range from $100 to $1.5 million per each type of

violation per year, depending on the culpability and knowledge of the covered entity or business associate.[26] The OCR must assess any civil money penalty within six years from the date of occurrence of the violation.[27]

2. GINA

The Genetic Information Nondiscrimination Act of 2008 and its implementing regulations is a federal law designed to protect individuals from discrimination based on their genetic information in the context of health insurance and employment.[28] Specifically, GINA prohibits certain insurance industry entities from requiring enrollees or their family members to undergo genetic testing, and from using genetic information in connection with underwriting and certain other insurance functions.[29] GINA also prohibits certain employers from using, disclosing or requesting employees' or job applicants' genetic information for employment-related purposes.[30] GINA defines "genetic information" broadly to include not only an individual's genetic tests, but those of the individual's family members as well as the "manifestation of disease or disorder in family members …."[31]

GINA regulates discrete categories of entities, such as group health plans, health insurance issuers, and employers with fifteen or more employees, in their conduct of specific kinds of activities. While its scope is circumscribed in this regard, GINA's requirements and restrictions on the collection, use and disclosure of genetic information are such that policies, procedures and training are operationally important to support compliance by entities that must comply with GINA. For example, such policies and procedures are important to assure entities subject to GINA do not use genetic information for prohibited purposes not necessarily prohibited under HIPAA or other privacy laws.

3. 42 C.F.R. Part 2

The federal confidentiality of substance abuse patient records statute, section 543 of the Public Health Service Act,[32] and its implementing regulations, 42 C.F.R. Part 2, as amended and referred to as "Part 2", protect the confidentiality of substance use disorder patient records generated or maintained by a federally assisted program providing substance use disorder diagnosis, treatment or referral for treatment.[33] The statute was enacted in 1974 in response to discrimination associated with substance use disorders and the fear of seeking treatment due to possible prosecution.[34]

Part 2, similar to HIPAA, protects substance use disorder records by specifying the circumstances under which such records may be disclosed. However, Part 2 is more restrictive than HIPAA as it has more robust consent requirements and specific rules regarding court orders prior to disclosure or use of any substance use disorder records.[35] While Part 2 has undergone amendment to align more closely with HIPAA, disclosures of substance use disorder records may only be made with written patient consent or if an exception applies, such as a medical emergency or for research purposes, with requirements that must be met for each such exception.[36] Among other things, the written consent must specify the name of the recipient individual or entity, the purpose of the disclosure and the date, event or condition upon which the consent will expire.[37] Moreover, further redisclosure of the substance use disorder records is generally prohibited unless expressly permitted by written consent.

The applicability of Part 2 extends beyond Part 2 programs and imposes requirements on other "lawful holders"[38] of substance use disorder records, such as a qualified service

organization. A QSO is any individual or organization that provides services to a Part 2 program that has entered into a written agreement stating the QSO will meet Part 2 requirements and will resist requests as part of judicial proceedings for SUD records.[39]

Hospitals or clinicians that are not Part 2 programs in the scope of their practice may obtain PHI related to substance use disorders directly from patients. This information is not subject to Part 2.[40] However, that same hospital or clinician may receive substance use disorder records from a Part 2 program, which are subject to Part 2. Given this, segregation, segmentation or labeling of Part 2 records may be required for some organizations for Part 2 compliance.[41] By extension, any business associate receiving both PHI and Part 2 substance use disorder information from a covered entity may also need to ensure the two types of information remain separated. As the health industry and health information heads toward further digitization, the norm of maintaining Part 2 records in paper format for segregation purposes may no longer be feasible. This means that to the extent an organization receives Part 2 records, the privacy function, as part of its role, must consider policies and processes for appropriate segregation or segmentation of Part 2 records from other PHI.

For providers, the use of certified electronic health record technology provides a mechanism to achieve this. The "data segmentation for privacy," or DS4P, certification criteria for certified electronic health record systems supports functionalities for a more granular approach to tagging data. While tagging capabilities are not explicitly required for the electronic exchange of Part 2 records at this time, regulatory efforts to provide patients with more control over their Part 2 records may mean organizations should be prepared to respond to specialized requests by patients related to Part 2 records. As an example, the Coronavirus Aid, Relief, and Economic Security Act provides patients with the right to request a restriction on the use or disclosure of SUD records for treatment, payment or healthcare operations. Accordingly, the privacy function should evaluate the benefits of electronic tools to help meet current and future privacy obligations related to Part 2.

4. Interoperability and information blocking

When passed in 2009, the Health Information Technology for Economic and Clinical Health Act incentivized the adoption and use of health IT through incentive payments under the Medicare and Medicaid programs to eligible providers. The Patient Protection and Affordable Care Act, enacted in 2010, continued this adoption through reimbursement policies and value-based payment programs that required further use of health IT and health information exchange capabilities. As a result, while there was prolific adoption of health IT, there was a lack of interoperability between these systems and tools.

In 2016, Congress passed the 21st Century Cures Act[42] to, among other things, increase interoperability and electronic access to and exchange of health information. This was codified into two sets of regulations. First, the Final Rule by the Office of the National Coordinator for Health Information Technology, as amended, introduced new requirements for developers of EHRs or certified health IT related to the exchange of health information and established rules to prevent "information blocking." Second, the Final Rule from the Centers for Medicare and Medicaid Services required measures to allow for the transition of health information such that patients can move from payer to payer or provider to provider with their health information transitioning along with them. These regulations are relevant to health privacy

because plans, providers, health information networks or exchanges, EHRs and other developers of health IT will need to strike a balance between preserving privacy in accordance with privacy laws while ensuring health information is shared in compliance with these interoperability and information blocking regulations.

5. Specific state laws

For entities that collect or otherwise process personal information of individuals who are from multiple states, developing a privacy compliance function that addresses all applicable state law requirements in addition to requirements under federal law can be a particularly complex endeavor. This is because HIPAA does not preempt state law to the extent the state law: (1) is not "contrary" to HIPAA[43] and (2) relates to the privacy of individually identifiable health information and is more stringent than HIPAA.[44]

Certain states have enacted extensive laws that restrict how health information may be used and disclosed.[45] In addition, many states have enacted myriad privacy laws that protect specific categories of sensitive health information, such as mental health records[46] and sexually transmitted infections and diseases.[47] While these laws vary extensively, their applicability is sometimes limited to specific entities, such as certain licensed healthcare providers or professionals, or entities that provide services to such providers. Some laws regulate the extent to which entities may disclose information without consent or authorization of the individual and may establish certain rights of data subjects with respect to their information, such as the right of access.

By way of example, state genetic privacy laws include restrictions on the performance of genetic testing and the collection, retention, use and sharing of genetic information or biospecimens that are collected for the purpose of genetic testing.[48] Whereas HIPAA permits a covered entity or business associate to use and disclose PHI without a HIPAA authorization for a number of purposes, such as the covered entity's payment activities, quality assessment or for research (all subject to certain conditions), many state genetic privacy laws do not include exceptions to their consent requirements for the use and sharing of genetic information or biospecimens that align with those under HIPAA. As a result, establishing internal policies and procedures for the management of genetic information that support compliance with applicable state and federal law while not being overly complex and impractical requires careful consideration by legal, business, and IT stakeholders.

In addition, as of the date of publication, three states have enacted laws that establish privacy protections specifically for biometric information.[49] Other jurisdictions address biometric data in the context of breach notification laws,[50] broader privacy and data protection laws,[51] and requirements relating to the use of facial recognition technology.[52] Biometric privacy laws may require organizations to refrain from collecting biometric data unless they comply with certain requirements such as prior written notice to the individual of the biometric data collection and the period of retention that applies to such data. Such laws also restrict the extent to which organizations may disclose or retain biometric data and impose requirements for safeguarding such information from unauthorized access or use.

In addition, many states have enacted laws that specifically protect certain information relating to minors. Such laws may require consent or authorization from the minor prior to disclosure of the minor's health information to a parent or guardian, particularly with

respect to sensitive health information such as alcohol or substance abuse treatment information, family planning information, and mental health information.[53] These laws also intersect with other state laws that establish when a minor is able to consent to medical care related to the subject of such protected personal information.

B. Consumer protection laws

The United States is generally regarded as a "sectoral" jurisdiction with respect to data privacy regulation. This means privacy laws in the U.S. are not comprehensive in their applicability but rather apply to particular industry sectors, such as healthcare (HIPAA) or financial services (Gramm-Leach-Bliley Act). However, these sector-specific laws are overlaid by state and federal regulations that apply more broadly to consumers' personal information and certain activities involving consumers' personal information. Collectively, we refer to such laws as "consumer protection" laws.

Consumer protection laws may be "additive" in that a consumer protection law and sectoral law both apply to the same information. For example, with respect to health information, a HIPAA-covered entity must obtain individual authorization prior to using or disclosing health information for activities that are not treatment, payment or healthcare operations activities, or for other purposes permitted or required by the HIPAA Privacy Rule. However, the Federal Trade Commission Act also applies, and it prohibits companies, including HIPAA covered entities, from engaging in deceptive or unfair acts or practices in or affecting commerce, including misleading consumers about what is happening with their health information. Thus, a HIPAA-covered entity must ensure both its HIPAA authorization satisfies the HIPAA Privacy Rule's content requirements and the information surrounding the HIPAA authorization does not create a deceptive or misleading impression in violation of the FTC Act.[54]

In addition, consumer protection laws may contain exemptions or carve-outs for information separately regulated by a sectoral law. For example, the California Consumer Privacy Act contains "exceptions" for medical information governed by the California Confidentiality of Medical Information Act and PHI governed by HIPAA,[55] and state personal information breach notification laws sometimes contain exemptions or "deemed compliance" provisions for HIPAA covered entities and business associates. A few particularly important consumer protection laws bearing on data privacy and protection are discussed below.

1. FTC

The Federal Trade Commission is the primary U.S. federal enforcement agency with respect to consumer privacy and security matters for most businesses.[56] The FTC has brought legal actions against organizations for violations of consumers' privacy rights, misleading consumers by failing to maintain security for sensitive consumer information and causing substantial consumer injury.[57] In these cases, the FTC frequently relies on its enforcement authority under Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices in or affecting commerce.[58] The FTC's enforcement authority also includes key portions of the Fair Credit Reporting Act,[59] the Gramm-Leach-Bliley Act[60] and the Children's Online Privacy Protection Act of 1998.[61]

The FTC has also promulgated a Health Breach Notification Rule that requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information.[62] In addition, if a service provider to one of

these entities has a breach, it must notify the entity, which in turn must notify consumers.[63] The FTC Health Breach Notification Rule does not apply to HIPAA-covered entities or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity,[64] which are governed by the HIPAA Breach Notification Rule.[65]

In January 2021, the FTC exercised its enforcement authority and provided clarity on its approach to health information privacy through its settlement with Flo Health. By way of background, via the Flo Health's mobile app, the Flo Period & Ovulation Tracker, consumers were able to share data about their gynecological health, including information about physical health, menstruation, pregnancy and childbirth. The FTC filed a complaint against Flo Health alleging the company shared this information with third parties without individual consent and without setting limitations on how the third parties may use this information.[66] Flo Health's privacy notices, however, stated the app would not share users' health information with others.[67]

The FTC's settlement with Flo Health provides some insight into how the agency may address practices related to health information moving forward. As part of the settlement, Flo Health is required to inform users about the purposes of data collection, use and disclosure, and inform consumers about controls they may exercise over their data.[68] In addition, Flo Health must identify the parties to whom health information may be disclosed, the categories of health information disclosed to such third parties and the purposes of such disclosure, including how the information may be used by the third party.[69] Importantly, Flo Health must now obtain a user's affirmative express consent prior to sharing information with third parties.[70]

Specifically, healthcare providers may utilize what is commonly referred to as the "healthcare messages exemption" to the TCPA, which permits healthcare providers to transmit such messages without the patient's prior express consent in order to convey important informational "healthcare messages."

2. TCPA

The Telephone Consumer Protection Act[71] and its implementing regulations[72] restrict telephone solicitations and the use of automated telephone equipment.[73] The TCPA limits the use of automatic dialing systems, artificial or prerecorded voice messages, SMS text messages and fax machines. It also specifies several technical requirements for fax machines, autodialers and voice messaging systems — principally with provisions requiring identification and contact information of the entity using the device to be contained in the message.[74] The TCPA allows for actual damages or statutory damages ranging between $500 per violation and treble damages up to $1,500 per violation for willful or knowing violations.

Of particular relevance in the healthcare context, certain exemptions exist to the TCPA's generally applicable prior express written consent requirement for transmitting artificial or prerecorded voice calls to cell phones or SMS messages. Specifically, healthcare providers may utilize what is commonly referred to as the "healthcare messages exemption" to the TCPA, which permits healthcare providers to transmit such messages without the patient's prior express consent in order to convey important informational "healthcare messages." Examples of

such messages might include appointment confirmations, prescription notifications and exam reminders. However, use of the "health-care messages exemption" entails a number of underappreciated restrictions, including that patients cannot be charged for the call or SMS message, that no more than three such messages may be initiated per week, and the content of messages must be limited to permitted purposes and cannot include marketing or promotional consent.[75]

The TCPA is enforced by the Federal Communications Commission, which may take administrative action, including imposing civil monetary penalties.[76] State attorneys general and other state officials or agencies may bring a civil lawsuit in federal court for injunctive relief and damages in the amount of $500 for each violation, which may be trebled if the court finds the defendant acted willfully or knowingly.[77] In addition, the TCPA provides a private right of action, and federal and state courts share concurrent jurisdiction over claims arising under the TCPA.[78] TCPA suits commonly generate uncapped statutory damages awards and class settlements in the tens of millions of dollars — even where the violation is not intentional.

3. CAN-SPAM

The Controlling the Assault of Non-Solicited Pornography And Marketing Act[79] and its implementing regulations[80] establishes requirements for commercial electronic mail messages and gives recipients the right to opt out of such communications. The CAN-SPAM Act defines "Commercial Electronic Mail Messages" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."[81] The CAN-SPAM Act makes no exception for business-to-business email. The CAN-SPAM Act is enforced by the FTC. Each separate email in violation of the CAN-SPAM Act is subject to penalties up to $43,792.[82]

4. CCPA and similar state laws

The California Consumer Privacy Act[83] and its implementing regulations[84] is a comprehensive consumer privacy law that took effect on Jan. 1, 2020, and regulates how certain for-profit businesses that do business in California collect, use and disclose the personal information of consumers who reside in California. Among other things, the CCPA confers to California consumers: the right to receive notice of the categories of personal information to be collected by a business, how the business will use and share the personal information, and the third parties who will receive the personal information;[85] the rights to access,[86] delete[87] or transfer personal information;[88] the right to opt out of the "sale" of personal information;[89] and the right to receive equal service and pricing from a business after exercising a consumer right granted by the CCPA.[90] Other states have enacted or proposed consumer privacy legislation similar to the CCPA[91] and the requirements of the CCPA are generally viewed as the most restrictive with respect to consumer personal information.

The CCPA does not apply to personal information that is PHI collected by a covered entity or business associate governed by HIPAA. The CCPA also does not apply to a covered entity governed by HIPAA to the extent that the covered entity maintains patient information in the same manner as PHI.[92] HIPAA-covered entities and business associates are still subject to the CCPA with respect to personal information they collect from California consumers that is neither PHI under HIPAA nor patient information that a covered entity maintains in the same manner as PHI.

Violations of the CCPA are subject to enforcement by the California attorney general's office, which can seek civil penalties of $2,500 for each violation or $7,500 for each intentional violation after notice and a 30-day opportunity to cure have been provided.[93] In addition, private plaintiffs may bring a civil action against a business in the event of a data security breach that results in unauthorized access and exfiltration, theft, or disclosure of the individual's personal information if the breach is attributable to a failure to implement reasonable security procedures and practices appropriate to the nature of the personal information at issue.[94] The statute allows for recovery of up to $750 per consumer, per incident or actual damages, whichever is greater.[95]

C. Human subject protection requirements

Privacy requirements also arise from laws and regulations relating to the conduct of human subjects research. These laws and regulations establish protections for the individuals who participate in biomedical and other research, which may occur simply by virtue of the use of their identifiable information for the purpose of research.[96] While the focus of these laws is not limited to privacy, they require regulated entities to address data subject confidentiality and privacy as part of an overall mandate to protect the welfare and interests of individuals who participate in research.

Human subject protection laws and regulations have been enacted and implemented at the federal and state level. The key federal regulations setting forth human protection requirements are the Federal Policy for the Protection of Human Subjects, also known as the "Common Rule," and U.S. Food and Drug Administration regulations. The Common Rule applies to non-exempt human subjects research that is conducted, supported or otherwise subject to regulation by any federal department or agency that has taken appropriate administrative action to apply the Common Rule to such research (including the U.S. Department of Health and Human Services).[97] FDA good clinical practice regulations apply to "clinical investigations," which generally mean "any experiment that involves a test article and one or more human subjects and that either is subject to requirements for prior submission to [FDA]" or where the results of such an experiment "are intended to be later submitted to, or held for inspection by, [FDA] as part of an application for a research or marketing permit."[98] In addition, certain states, including California,[99] Maryland[100] and New York[101] have enacted human subject protection laws.

Both the Common Rule and FDA GCP regulations include institutional review board review and informed consent requirements for the research they regulate, which restrict how identifiable information of a study subject may be collected, used and disclosed for research purposes. The standards under the Common Rule and FDA GCP regulations regarding when informed consent is required, when IRB waiver or alteration of informed consent is permitted, and when an IRB may approve a proposed study based on its assessment of specified criteria (including the risks presented to subjects' privacy and confidentiality) closely relate to and must be implemented in coordination with any privacy laws that also apply to the regulated studies. Likewise, an organization's approach for complying with applicable privacy laws must be coordinated with its compliance approach for any applicable state human subject protection laws — some of which incorporate the requirements of the Common Rule or FDA GCP regulations[102] or apply to a study only if the study is not subject to the Common Rule and FDA GCP regulations.[103]

D. Foreign and international corollaries

There are two general "models" for data privacy and protection regulation. The first approach, referred to as the "sectoral" approach, is a sector-specific or industry-specific approach. The U.S. has largely implemented a "sectoral" approach in which, for example, the health sector is generally regulated by HIPAA and the financial sector is generally regulated by GLBA. The second approach, referred to as the "omnibus" approach, applies broadly across all or most sectors or industries. The European Union has largely implemented an omnibus approach through the EU's General Data Protection Regulation, as discussed below.

We discuss below at a high level the contours of data privacy and protection regulation in certain jurisdictions outside the United States that are generally regarded as having among the most restrictive requirements or in our experience are among the most relevant for US-based healthcare industry organizations doing business abroad.

1. European Union

The General Data Protection Regulation is an omnibus regulation on data protection and privacy in European Economic Area. The GDPR's primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[104]

The GDPR defines "personal data" quite broadly, including any information relating to natural persons who: (i) can be identified or who are identifiable, directly from the information in question; or (ii) who can be indirectly identified from that information in combination with other information.[105] Personal data does not include data that has been "anonymised" in accordance with the GDPR's requirements.[106] Under the GDPR, "data controllers" and "data processors" have certain responsibilities with respect to personal data and demonstrating compliance with the GDPR's data protection principles.

A data controller is a legal or natural person, agency, public authority or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it.[107] A data processor is a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of a data controller.[108]

The GDPR has extraterritorial effect and contains robust provisions and requirements related to the processing of personal data. Each member state has enacted supplementary legislation to ensure the GDPR works within the relevant national legal framework.

As of Dec. 31, 2020, the United Kingdom is no longer subject to EU law. Therefore, the GDPR will be brought into U.K. law as the "U.K. GDPR" via a statutory instrument that will make technical amendments to the GDPR so it works in a U.K.-only context.

Within the EU, there are also national laws that provide additional controls around the processing of health data.

Under the GDPR, EU national authorities can or must assess fines for specific data protection violations in accordance with the GDPR. The fines are applied in addition to or instead of further remedies or corrective powers, such as the order to end a violation or an instruction to adjust the data processing to comply with the GDPR, as well as the power to impose a temporary or definitive limitation including a ban on data processing. The GDPR establishes two tiers of fines based on the severity of the violation.

> ***As of Dec. 31, 2020, the United Kingdom is no longer subject to EU law. Therefore, the GDPR will be brought into U.K. law as the "U.K. GDPR" via a statutory instrument that will make technical amendments to the GDPR so it works in a U.K.-only context.***

Less severe violations could result in a fine of up to 10 million euros or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.[109] These violations include any violation of the articles governing data controllers and data processors, certification bodies and monitoring bodies.[110] More severe violations could result in a fine of up to 20 million euros or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.[111] These include any violations of the articles governing basic principles for processing, conditions for consent, data subjects' rights and transfer of data to an international organization or a recipient in a third country.[112]

Beyond just the text of the GDPR, the EU is actively soliciting feedback and formulating its approach to health data. In March 2021, the European Commission released the "Assessment of the EU Member States' rules on health data in light of the GDPR," which analyzes the differences in approaches to the processing of health data by member states and identifies potential EU level action for a uniform approach. In addition, the European Data Protection Board provided clarification on the application of GDPR on health research and, most recently, the European Commission opened a public consultation on the European Health Data Space to obtain feedback on the collection, access, use and reuse of health data. Organizations subject to the GDPR should remain informed of these developments to both adjust their approach to GDPR compliance and remain aware of new developments that may be followed in other jurisdictions.

2. Brazil

Brazil's General Data Protection Law[113] is an omnibus data protection law and is designed to enhance the privacy and protection of personal data of individuals in Brazil. The LGPD resembles the GDPR and, like the GDPR, has extraterritorial reach. The LGPD generally applies to any organization that processes personal data of individuals in Brazil regardless of where the organization is located and without regard to where the data is stored or otherwise processed, if: (1) the processing is carried out or collected in Brazil; (2) the purpose of the processing is to offer or provide goods or services to individuals in Brazil; or (3) the purpose of the processing is to process personal data of individuals in Brazil. The LGPD imposes GDPR-like requirements on controllers and processors of personal data, with greater protections for sensitive personal data. Organizations must have a legal basis to process such data. Data subjects in Brazil have a number of rights over their personal data, including rights of access, correction, anonymization, blocking and deletion of data, and portability, among others. Violation of the LGPD may result in significant administrative fines issued by Brazil's regulators.

3. Israel

Israel's data protection regime is governed primarily by the Protection of Privacy Law and the regulations promulgated under it, as well as[114] the guidelines of the applicable Israeli regulator, the Privacy Protection Authority. The PPL does not clearly state its jurisdictional scope. One interpretation is that the jurisdiction of the PPL is comparable

to that of other Israeli laws, i.e., limited to entities or acts within Israel. This would mean the PPL applies to: (1) database owners, database holders and database managers based in Israel; and (2) data processing operations that take place in Israel, regardless of whether the individuals about whom the data relates are residents or citizens of Israel. The PPL could also be interpreted to apply to non-Israeli database owners, database holders or database managers that process personal information about Israeli residents or citizens when such processing takes place outside of Israel, because the PPL does not explicitly define a database owner, database holder or database manager as an Israeli entity or other Israeli person. Various regulations promulgated under the PPL by the PPA set out rules and procedures for data security, data retention, data subject rights and cross-border transfers of data. These regulations also do not clearly state their jurisdictional scope, so they could extend to foreign-based entities that process data about Israeli citizens.

The PPA is required to maintain the Registry of Databases and is empowered to supervise compliance with and investigate alleged violations of the PPL and related regulations. The Administrative Offences Regulations permits the Registrar to impose administrative fines. In addition to administrative fines, offenders may also be charged with criminal liability and subject to up to five years in prison if the violation is committed willfully. A breach of privacy is actionable and an individual claimant may obtain monetary compensation or injunctive relief. A court may award statutory damages without proof of damages for breaches of privacy rights. If the breach was intentional the damages may be doubled. The PPL also specifies that an act or omission in breach of certain of its provisions (e.g., failure to ensure data security) may give rise to a tort claim.

4. Australia

Australia's federal Privacy Act 1988 and the 13 Australian Privacy Principles contained in the Privacy Act apply to government agencies and private sector organizations with annual turnover exceeding AU $3 million. The Privacy Act extends to all of Australia's external territories, but also applies to an act done, or practice engaged in or outside Australia (and Australia's external territories) by an organization or small business operator that has a link to Australia (i.e. continued presence, partnership, incorporation, central management and control, or citizenship in Australia). An organization may also have a link to Australia if the organization conducts business in Australia and collects or stores personal information in Australia.

A number of factors should be considered when determining whether an organization conducts business in Australia, including whether the organization (a) has a place of business in Australia, (b) employs individuals in Australia, (c) has a website that offers goods or services in Australia, (d) includes Australia in a drop-down list as an available country on the organization's website, (e) has web content that is part of the business or was uploaded by or on behalf of the entity in Australia, (f) fulfills business or purchase orders in Australia, or (g) is the registered owner of trademarks in Australia.

The Privacy Act applies to any collection, holding, use or disclosure of personal information by a regulated entity, with enhanced protections for sensitive information. The Privacy Act prescribes certain rights for individuals, including rights to know why the information is collected, how it is used and to whom it is disclosed, the right of the individual not to identify themselves in certain circumstances, the right of access, the right

to stop receiving unwanted direct marketing, the right to correct information and the right to make a complaint. Australia's Privacy Commissioner enforces the Privacy Act and any acts that may violate an individual's privacy. The Privacy Commissioner can levy significant fines on individuals and corporations that violate the Privacy Act.

5. Canada

Canada has several federal, provincial and territorial privacy statutes that govern the protection of personal information. The Personal Information Protection and Electronic Documents Act 2000 applies to the collection, use and disclosure of personal information in the course of commercial activities in Canada. Although PIPEDA is silent with respect to its extraterritorial application, the Federal Court of Canada concluded PIPEDA applies to businesses established in other jurisdictions if there is a "real and substantial connection" between the organization's activities and Canada. PIPEDA does not apply to the collection, use or disclosure of employee information, except as related to federal work. However, provincial laws may apply. PIPEDA and provincial data protection laws require specific notices regarding openness and transparency, and require regulated organizations to obtain consent in order to process such information. Canadian individuals enjoy rights or access and to correct inaccuracies. Violations of Canadian data protection laws can result in significant fines.

6. India

Other than the Indian Constitution, which was recently interpreted to include a fundamental right to privacy, India does not currently have a singular comprehensive law regulating the processing of personal data. Instead, India's laws and regulations address specific sectoral data protection concerns. The Information Technology Act 2000 (as amended) is the primary national law regulating the collection and use of personal information that is sensitive. The IT Act applies to corporations and other "body corporates" that possess, maintain, or otherwise process personal information, including body corporates that act on behalf of other body corporates. Certain provisions of the IT Act provide liability for negligent handling of personal information. For example, the IT Act provides that any corporation or other body corporate that handles sensitive personal data is liable to pay damages for any loss caused by its negligence in implementing and maintaining reasonable security practices and procedures. While the IT Act by its language appears to apply extraterritorially, the practical implications of such language appear limited.

The corresponding Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Data Privacy Rules) were issued under the IT Act and regulate the use of personal information and sensitive personal data. The Data Privacy Rules mandate that businesses have a privacy policy, obtain consent when collecting or transferring personal information, and inform the data subject about any recipients of that data. The government of India clarified that the Data Privacy Rules apply only to entities located in India. However, where an Indian entity directly collects personal data from individuals, the Data Privacy Rules apply regardless of whether the individual is based in India. The IT Act includes a private right of action for individuals, as well authorizing criminal punishment (with a fine or three years in prison or both) for disclosing personal information without the consent of the data subject or in breach of any relevant contract.

E. Certifications and standards

In addition to complying with legal and regulatory requirements, healthcare companies may voluntarily obtain privacy or security certifications or accreditations or comply with additional standards that are helpful in the marketplace or are required by contract. Healthcare companies may also undertake to comply with self-regulatory industry regimes. This section provides an overview of certain certifications, accreditations, standards and self-regulatory regimes that are particularly relevant in the healthcare sector.

1. PCI-DSS

The Payment Card Industry Data Security Standard was issued by the Payment Card Industry Security Standards Council and establishes industry standards for the processing of payment card information. While the PCI-DSS requirements do not have the force of law, the penalties for noncompliance could include exclusion from payment card systems.

2. HITRUST CSF

The HITRUST CSF is a certifiable framework that provides organizations with a detailed approach to data security compliance and risk management. The HITRUST CSF incorporates healthcare-specific security, privacy and other regulatory requirements from HIPAA, PCI-DSS, ISO/IEC 27001 information security management standards and Minimum Acceptable Risk Standards for Exchanges. HITRUST offers three degrees of assurance, or levels of assessment: self-assessment, CSF-validated and CSF-certified. Each level builds with increasing rigor on the one below it. HITRUST certification may be a requirement, or heavily favored, for doing business with certain healthcare companies, such as health plans.

3. SOC 2

A SOC 2 audit report is designed to provide assurance to service organizations' clients, management and user entities about the suitability and effectiveness of the service organization's privacy and security controls. The SOC 2 auditing and reporting process is guided by a framework called the Trust Service Criteria. The TSC is built upon five criteria: (1) security; (2) availability; (3) processing integrity; (4) confidentiality; (5) privacy.

There are two types of SOC 2 audits. A SOC 2 Type I audit examines the controls that service organizations use to address any or all five of the TSC. This audit type describes the service organization's systems and provides assurance that controls are effectively designed to meet relevant trust criteria at a specific point in time. A SOC 2 Type II audit includes additional attestation that a service organization's controls undergo testing for operating effectiveness over a period of time. User organizations and their auditing team often select six months for the period of time to evaluate.

Organizations undergoing a SOC 2 audit often include those that provide services such as data hosting, co-location, data processing, cloud storage and software-as-a-service. SOC 2 audits may be performed as part of a regular security program or if the user organization suspects there is a data security issue with one or more of the TSC at the service organization.

4. ISO 27000 Series

The International Organization for Standardization is an international organization that develops consensus-based standards in several functional areas, including information technology security standards. In collaboration with the International Electrotechnical Commission, the ISO 27000 series

was developed with the intent to identify objectives, controls, requirements and guidelines for effective information security.[115] The series itself contains numerous standards addressing different aspects of information security, but the ISO 27001 standard specifies the general requirements for information security management, while ISO 27006 contains the requirements for certification bodies that perform audits to verify organizations are conforming with the requirements of ISO 27001. Other notable guidance-based standards include ISO 27000 (Overview and Vocabulary), ISO 27002 (Code of Practice for Information Security Controls), ISO 27003 (Guidance for Implementation), ISO 27005 (Risk Management), ISO 27014 (Information Security Governance), ISO 27032 (Cybersecurity) and ISO 27799 (Information Security Management in Health).

The standards within the ISO 27000 series are process-oriented and follow a plan-do-check-act approach:

- Plan: Identify types of information and associated security requirements, assess information security risks and select controls to manage risks.
- Do: Implement controls and manage operations for the information security management system.
- Check: Monitor and assess performance of the information security management system.
- Act: Take any corrective or preventive actions necessary for maintenance and improvement.[116]

This approach is taken for several domains, including asset management, physical and environmental security, access control, information security incident management and business continuity management.[117] In addition, organizations are expected to maintain structured and organized documentation that speaks to things like change or approval processes and rules for information access and protection.[118]

> ***When organizations undergo an ISO audit by an authorized certification organization, they provide documentation in advance showing policies, processes and other relevant information, which the auditors review prior to an on-site visit.***

Similar to other certifications, when organizations undergo an ISO audit by an authorized certification organization, they provide documentation in advance showing policies, processes and other relevant information, which the auditors review prior to an on-site visit. The on-site visit may include interviews with relevant stakeholders as well as technical review of the various controls. Upon conclusion of the audit, the certification organization provides a report identifying any recommendations for improvement and, in the event of a successful audit, an official certificate with supporting documentation speaking to the organization's compliance with requirements of the standard. This certification lasts three years with annual monitoring.[119]

III. Healthcare privacy program pillars

Against the legal backdrop described in Section II, this Section describes the proposed components of an organization's healthcare privacy function. To implement an organi-

zation's compliance with applicable privacy laws, regulations and standards, and to facilitate a coordinated approach between privacy and security, this article recommends the following pillars of a privacy function: (A) Legal Analysis, (B) Policies, Procedures and Guidelines, (C) Contracting, (D) Product Counseling, (E) Privacy Operations, (F) Privacy Risk Assessments, (G) Security Coordination and (H) Coordination with Other Regulatory and Compliance Functions. Within each pillar, we describe a set of core activities that comprise the pillar.

This framework is not the exclusive way to approach a privacy program. In addition, not all of the activities discussed below are necessarily appropriate for every healthcare organization, and certain organizations may find it helpful to incorporate additional functions in its privacy program that are not outlined here. The utility of a particular activity and the level at which it is performed will depend on many factors, including the maturity and size of the organization, the size of the privacy function, the kinds of data the organization processes, where the organization operates, its risk tolerance and the key imperatives driving the business.

A. Legal analysis

A privacy function serves as the key resource for the company on the privacy requirements that apply to a company's processing of personal information. Key responsibilities in this regard include:

1. Analyzing and providing guidance on applicable laws

A privacy function should support the legal analysis of the privacy and data protection laws, regulations and standards that apply to the company and what they require. Below are key privacy and related laws that may apply to a healthcare entity's processing of personal information, along with an illustrative list of common gating questions and issues that arise under these laws.

HIPAA:

- Evaluate whether a company is a covered entity, business associate, or both. This informs the permissibility of any given use or disclosure of PHI. In the case of a covered entity, the organization should have policies and processes in place to assess whether a proposed use or disclosure is for treatment, payment, healthcare operations or another purpose for which HIPAA authorization is not required. In the case of payment or healthcare operations, covered entities should also assess how best to meet the minimum necessary requirement.[120] For business associates, assessing proposed uses or disclosures of PHI should include a review of the applicable business associate agreement[121] and underlying services or other agreement with the covered entity to determine if and how PHI may be used and disclosed. For instance, if the business associate would like to deidentify PHI for its use case, it should assess whether it has retained the ability to deidentify the PHI within its business associate agreement.

- Identify and help implement appropriate pathways under HIPAA for a company's (i) "primary" uses and disclosures of PHI (such as treatment and payment functions for an organization that is a covered entity, and the provision of services to a covered entity or upstream business associate customer where the organization is a business associate), and (ii) a company's various "secondary use" activities that require access to PHI received in connection with primary uses and disclosures, such as research, product development and quality improvement.

- Advise on other permissible uses and disclosures of PHI, such as in connection with marketing initiatives.

- Advise on a company's compliance obligations under HIPAA, including with respect to the minimum necessary requirement, third party requests for PHI, use of e-mail to send PHI, and the scope of an individual's right to access, amendment and accounting of disclosures with respect to PHI.

- Advise on standards for deidentification, data aggregation and creating limited data sets.

GDPR and other multinational or international privacy laws:
- Evaluate a company's role as a controller vs. processor, as GDPR obligations will vary depending on the role.

- Identify and implement bases for processing for primary and secondary data use activities. (This will have some overlap with HIPAA but the analysis will be distinct.)

- Analyze international data transfer issues. In particular, the privacy function should analyze all proposed data flows from the EEA to facilitate compliant cross-border data transfers, such as through EU Commission-approved standard contractual clauses where appropriate.

- Advise on standards for pseudonymization and anonymization of personal data.

- Address other international privacy laws that bear upon how a company conducts its business and collects, uses or discloses personal information.

U.S. state privacy laws:
- Analyze the extent to which state privacy laws are more protective of privacy and are not preempted by HIPAA.

Marketing laws:
- Analyze the applicability of marketing restrictions under HIPAA, GDPR, and laws such as the TCPA and CAN-SPAM Act to proposed communications by the business teams.

- Address compliance with website tracking requirements (e.g., cookie laws).

Privacy protections for employees:
- Analyze the applicability of various federal, state and other laws regarding the confidentiality, collection, use, disclosure and transfer of employees' personal information, such as the Americans with Disabilities Act, the Genetic Information Nondiscrimination Act, state consumer privacy laws (such as the CCPA), state data security laws, state breach notification laws and state laws on workplace surveillance.

Human subject protection laws that intersect with privacy laws
- Analyze activities involving the collection, retention, use and disclosure of personal information for research purposes under human subject protection laws, including laws with respect to the retention of human tissues.

- Ensure that proposed research activities align with applicable informed consent forms, contracts and other requirements and restrictions under applicable privacy and human subject protection laws.

2. Drafting legal memos

In some circumstances, it may be appropriate for the analysis conducted by a privacy function to be documented in legal memoranda or other written work product. This may help preserve the analysis for posterity and to support compliance going forward, such as where the analysis is an overview of a new key regulation or an overview of the legal framework that applies to a new product offering.

These legal memoranda can take several forms: (i) a legal opinion from outside counsel to understand new developments, application of law to a specific fact pattern, or guidance prior to making a specific decision, (ii) internal memoranda (typically known as a "Memo to File") to capture rationale for a particular decision, or (iii) a memoranda for business executives on considerations for decision-making. When drafting memos for business stakeholders, consider presenting the guidance in the form of different options to choose from, along with an analysis of the pros and cons of each option. This approach can empower the non-legal stakeholders to help craft a solution that addresses privacy requirements rather than mandating a particular approach. Note, however, that some business stakeholders may prefer to know the recommendation of the privacy function to help in their decision-making.

> ***To monitor developments, a privacy function can sign up for key regulators' listservs, client alerts from outside counsel, and key trade press and other industry publications and consider joining organizations and professional associations that focus on privacy.***

In large organizations, it may be useful to create a repository of memos with a brief explanation on content. This way, the information and analysis transcends personnel changes and foundational information can be leveraged if there are budget or time constraints to consider.

3. Monitoring legal developments

A privacy function monitors legal developments and keeps company stakeholders apprised of such developments. To monitor developments, a privacy function can sign up for key regulators' listservs, client alerts from outside counsel, and key trade press and other industry publications and consider joining organizations and professional associations that focus on privacy. Illustrative examples include:

- Outside counsel listservs.
- OCR privacy and security listservs.[122]
- Membership in the American Health Lawyers Association, International Association of Privacy Professionals or similar organizations.
- Cybersecurity and Privacy Law360 (currently a paid subscription).
- Practical Law (currently a paid subscription).
- Healthcare Info Security.[123]
- Social media (e.g., Twitter) accounts of regulators and privacy subject matter experts, such as the U.K. Information Commissioner's Office, EU Data Protection Authorities, @HealthPriv, Chris Hoofnagle (@hoofnagle), Lucia Savage (@savagelucia), Paul Schwartz (@paulmschwartz), and Daniel Solove (@DanielSolove).

- Reviewing guidance from influential EU bodies, such as the European Data Protection Board[124] and European Data Protection Supervisor's website.[125]

- Attending conferences such as those of IAPP, Privacy and Security Forum, HIMSS and AHLA.

B. Policies, procedures, and guidelines

A key component of privacy compliance is the set of internal policies, procedures, guidelines, checklists and other guidance documents that outline the privacy requirements applicable to a company. These materials inform company stakeholders what must be done to comply with obligations under applicable privacy laws, operationalize the requirements, and provide user-friendly guidance to key business and other stakeholders responsible for complying with such laws.

At a high level, we think there are three types of documentation that compromise this pillar:

- Policies and procedures that map closely to legal requirements also play a role in helping a company quickly and easily demonstrate to regulators, customers and other business partners (such as during an audit or a regulatory investigation) that a company has a privacy program that complies with applicable laws and regulations.

- Checklists, FAQs and other guidance documents present a set of shorter, more practical set of tools that can help further educate business personnel, contextualize the requirements for them and promote compliance. They should be consistent with the policies and procedures but are written in language that is less legalistic and more business-friendly and practical.

- Certain laws require external notices to patients and consumers to inform them of their privacy rights and how their personal information may be collected, used and disclosed.

1. Internal policies and procedures

Certain laws and regulations, including HIPAA and the GDPR, include specific requirements to implement policies and procedures. In addition, some policies and procedures may be helpful — if not required — in supporting a company's compliance with applicable legal requirements. One way to structure policies and procedures is to have a "Global Privacy Program" (or similarly structured document) that provides an overall roadmap for the privacy program and an overview of all policies and procedures under the program. Accompanying the roadmap document are specific policies and procedures reflecting and implementing the laws and regulations of the various jurisdictions in which a company operates. For example, there could be a specific policy on HIPAA and a separate policy on GDPR and other international laws that follow GDPR's framework. These separate policies can help a company quickly and easily demonstrate to a regulator or other third party that a company has satisfied a requirement to have a particular policy or procedure in place.

Even where a law does not specifically require a policy or procedure, it may be helpful to implement an overarching policy to formalize the requirements with which a company must comply. The privacy function should ensure that it periodically reviews its policies and procedures and updates them, as needed, in response to regulatory or organizational changes.

2. Checklists and other tools

A privacy function should lead the development of checklists, FAQs and other tools that translate privacy requirements into practical terms that are readily understandable by business team members and other non-legal personnel.

While policies are important, they are frequently not written in terms that can be readily applied by business teams. To meet this need, checklists and FAQs can serve as a critical bridge between the privacy requirements and the people who are supposed to follow the requirements. Atul Gawande has written persuasively about the importance of checklists in a range of disciplines, including construction and medicine.[126] Checklists can be an important tool for in-house counsel, as well.

A good checklist distills the legal requirements into concise bullet points that can be understood and implemented by business users. All extraneous information should be removed from checklists as should any privacy jargon or legalistic language. The checklists are most effective if they are targeted to particular teams or activities and are drafted in coordination with the users of the checklists. Checklists may include, by way of example:

- Checklist on Privacy Principles for Product Design — Addresses items such as purpose limitation, general data security and individual rights.

- Checklist on Patient or Consumer Outreach via Email and Text — Describes consent, message content and other requirements for emailing or texting patients or consumers.

- Checklist on Deidentification and Anonymization — Outlines steps to ensure data is deidentified in accordance with HIPAA or pseudonymized or anonymized in accordance with GDPR.

- HIPAA Authorization Checklist — Covers what must be included in a valid HIPAA authorization and operational considerations related to obtaining and retaining completed authorization forms.

Checklists can be supplemented by FAQs addressing commonly raised internal questions or questions from customers, vendors or other third parties.

Frequently, organizations struggle with disseminating these resources or informing business stakeholders about checklists and other tools that can be leveraged. Consider whether it may be effective to present the checklists to the targeted users and to create a company webpage or SharePoint site to make all checklists available in one centralized location.

3. External privacy notices

A privacy function should lead the development and maintenance of privacy notices and other patient or consumer-facing materials. Key examples include:

- *HIPAA Notice of Privacy Practices:* This document describes how a covered entity uses and discloses protected health information as well as certain patient rights with respect to protected health information. A copy of the document should be posted to the company website and in any patient-facing portals or applications.

- *External Privacy Policy:* The policy will inform individuals on how and why an entity uses and discloses personal information it obtains. This is a necessary transparency requirement under appli-

cable privacy law (e.g., FTC, GDPR) and is important in facilitating a company's ability to use personal information for its desired purposes. A privacy function should be the lead for drafting and revising the privacy notice.

- *CCPA Notice at Collection:* The CCPA requires that a business provide notice at or before the point of collection of the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.

- *Cookie Policies:* A cookie is a small piece of data stored on an individual's device when browsing the internet. Under EU data protection law and the CCPA, it is necessary to be transparent about what cookies are placed on individuals' devices. EU data protection law may also require obtaining consent for the use of such cookies. The privacy function should therefore:

  - Help prepare and maintain an up-to-date cookie policy to ensure that the cookies used by a company remain accurate.

  - Be mindful of developments in this area as a new EU regulation is set to come into force that will change the requirements for use of cookies in the EU.[127]

  - Ensure that appropriate consents are obtained (e.g., by way of a banner) where cookies are used, especially in relation to analytics or marketing cookies.

- *Marketing Consents:* Electronic marketing is heavily regulated in the EEA and other countries. In the U.S., the TCPA, CAN-SPAM Act, and state telemarketing laws regulate marketing communications made via calls, text, fax and email. It may therefore be necessary to obtain consents from individuals before providing them with direct marketing materials (e.g., offering certain products or services). A privacy function should provide input on the language that must be included when undertaking any marketing activities in relevant markets.

C. Contracting

A privacy function should support the drafting, review and negotiation of privacy-related provisions and contracts and privacy-related exhibits, as well as the diligence of potential vendors and other contractors.

1. Privacy contracting support for customer, vendor, and other contracts

A privacy function should advise on the contracts and terms that are necessary and appropriate for any collection, use, retention, or disclosure of data contemplated by the business, whether the contract is with a customer, vendor or other third party. For example, this includes advising on when a company must enter into a business associate agreement or data processing addendum with a third party or when specific mandatory language needs to be implemented with a data processor in line with GDPR requirements.[128] In some instances, the privacy function may be expected to negotiate with customers, vendors or other third parties on privacy-related matters in contract negotiations.

More generally, a privacy function advises on proposed arrangements with third parties to determine if the arrangement is permissible under applicable privacy laws.

2. Template privacy contracts

A privacy function should oversee the development and negotiation of any templates designed to satisfy requirements under privacy laws and that are necessary for the compliant use, disclosure, transfer or other processing of PHI, personal data or other personal information, such as:

- Business associate agreements (where a company is a covered entity, business associate, or downstream business associate).

- Data processing agreements, including in relation to data processing agreements with data processors (as required under Article 28 GDPR) and a company's requirements with respect to sub-processors.

- Standard contractual clauses (to legalize the transfer of EU data to the U.S.).

A privacy function should also have input into the development and negotiation of any other template agreements that relate to the collection, use, retention or disclosure of personal information, such as data license agreements and clinical trial agreements.

Insofar as a privacy function is not responsible for the development of the entirety of the above kinds of agreements, it should review templates with a focus on the following issues:

- Accurate and comprehensive citations to applicable privacy laws (e.g., in defined terms).

- Apportioning responsibility and liability in accordance with applicable privacy and data protection laws (e.g., will a company be acting as a covered entity, business associate, data controller, joint controller and/or data processor, who should be responsible for obtaining any necessary consents or authorizations, and does the agreement include appropriate restrictions on the third party's use of a company data, such as a prohibition against reidentifying any deidentified or anonymized data).

- Appropriate indemnification, limitation of liability and insurance coverage requirements (e.g., cyber or "breach" coverage) provisions (e.g., will a company seek indemnification for breaches of PHI or personal data that are not caused by negligence, willful misconduct, or violation of applicable law or the agreement, to what extent should the agreement limit liability relating to data breaches, and what insurance coverages, if any, should the other party by required to maintain).

- Appropriate and comprehensive representations and warranties by the third party (e.g., has the third party obtained all necessary rights, consents or authorizations to make available any data or otherwise perform its obligations under the agreement).

- Appropriate disclaimers by the company if it is responsible for providing data (e.g., of warranties regarding the data) and an understanding of the limitations of such disclaimers.

- Appropriate flow-down rights of a company with respect to downstream service providers or contractors in a company's agreement with its direct service providers.

3. Privacy contracting playbooks

For contracts that a company frequently needs to execute or issues that are often heavily negotiated, a privacy function can develop

contracting playbooks to promote standard negotiation approaches and help a company obtain terms that are as consistent as possible across all agreements. These playbooks may include:

- Preferred and fallback language.
- Talking points for the business and a company legal teams involved in negotiating the agreements.
- Certain deviations to standard language that need further privacy review.

4. Vendor diligence and oversight

A privacy function should coordinate with a company's security function to provide input into the company's diligence and ongoing oversight of vendors and other contractors (such as third parties to whom the company licenses data), and in some cases become directly involved in the diligence. Conversely, the privacy function of entities that are typically service providers to healthcare organizations should support the service provider's response to diligence requests, questionnaires, and audits and inspections. At its core, this role may relate to the following activities, and will depend on whether the entity is engaged in diligence or responding to such diligence:

- Obtaining, reviewing or responding to any information security questionnaires, security risk analyses, security audit reports and other reports that a contractor is required to provide.
- Conducting, overseeing or responding to audits to the extent permitted and appropriate under the contract.

The above activities are often handled by a security-focused team or a procurement group. However, privacy should be looped into such diligence to the extent there are privacy questions that arise during diligence. For example, a company may have an agreement with a cloud services provider or another provider of an essential information technology service. If the service provider reports a data breach or noncompliance with data privacy or security-related provisions under its agreement with a company, a privacy function should confirm whether such an event triggers the right of a company to conduct an audit of the vendor and conduct such an audit as a company deems appropriate.

Whether, in what manner, and how frequently such analyses and reports should be requested or provided will typically depend on the volume and sensitivity of the information involved and duration of access to the information by the vendor, which will inform the overall assessment of the vendor risk.

D. Product counseling

Incorporating privacy into the life cycle of a product or service is critical — from design and product development, to deployment, to re-designs and updates, and finally to ongoing evaluation and monitoring. A privacy function should lead the effort to embed privacy by design into the company's business.

To implement privacy by design, a privacy function needs to identify operating mechanisms to help integrate the privacy function into the product development life cycle, ideally at the early stages. Early privacy function input helps to ensure that the ultimate product or service delivered is consistent with applicable laws, contracts, and other requirements. In performing this responsibility, a privacy function should consider the following questions during each phase of the life cycle of the product, service, collaboration or initiative:

Phase 1: Product development

- What data is necessary for design/development of products and services?
    - What pathway would be used for any collection, use or disclosure of data?
    - Will there be data scraping or mining, or will public or government datasets be used? If so, are any preliminary steps required?
    - Is the organization prohibited by law or any contractual obligations from using the data for product development purposes?
    - What consents, authorizations or terms of use are needed, if any?
    - Is any secondary use of data for design and development purposes consistent with applicable consents, terms of use, agreements, notices, policies?
    - What licenses or agreements are necessary to obtain data necessary for design or development?
    - What data is collected, used, disclosed or retained in connection with development of the product, service, collaboration or initiative itself?
    - Are there any requisite privacy-by-design features that should be added during the design or development stage?
- How can the product, service, collaboration or initiative be developed in a way that facilitates privacy but does not impair functionality or design?
    - For example, query whether a clinical decision support tool needs to ingest parts of a medical record that includes a patient's payment information, email address or other contact information in order to provide the intended feedback to the contemplated user (e.g., a healthcare professional developing an appropriate treatment plan based on lab results).
- What are the specific purposes that the product, service, collaboration or initiative is designed to fulfill?
    - Restrict any uses or disclosures of personal information that are not necessary for these purposes.
    - Take a step back and query whether the uses and disclosures of personal information would be aligned with the expectations of the individual, the public and a regulator.
    - In the case of emerging technologies such as artificial intelligence, consider both input data and output data and any actions that may be necessary (e.g., if the output of an AI model results in the deidentification of PHI, is the organization permitted by the BAA or another agreement to do so?)
- What is the company's role with respect to the product/solution (e.g., controller or processor)?
    - Identify each of the individual rights that apply based on the company's role and nature of the product/solution.
    - Determine the processes and features that are necessary to implement the applicable individual rights. (E.g., how will individuals communicate with a company, what forms (if any) will be used, and what technical func-

tionalities such as data tagging are necessary?)

- Will the company seek to make any permitted secondary uses of the data, such as after identifiers have been removed?
  - Determine what secondary uses will be permitted and using what data.
  - If deidentified, anonymized or pseudonymized data will be used for secondary uses, confirm the company will have the necessary rights under applicable law, agreements, consents, terms of use, notices, etc. to create and use the deidentified, anonymized or pseudonymized data.

Phase 2: Product Deployment

- What agreements are necessary with customers, vendors or other third parties?
- To what personal information will any customer (other than an individual data subject), vendor, collaborator or other third party have access, and does such access align with applicable law, agreements, consents, terms of use, notices, etc.?
  - Ensure any necessary mechanisms (e.g., role-based access restrictions, establishment of separate databases, logs or disclosure tracking, etc.) are in place to manage third party access.
  - What consents, terms of use, notices, policies, etc. are needed?
  - Where will data be stored? How will the company's IT systems and infrastructure support privacy throughout the life cycle of the product, service, collaboration or initiative?
  - To the extent that the company determines that encryption is a reasonable and appropriate safeguard for the company under the HIPAA Security Rule's addressable implementation specifications, implement encryption for protected health information in transit and at rest.
  - Assess who will have access to personal information in connection with the product, service, collaboration or initiative, and implement user controls based on that assessment.
  - Implement data segregation, data tagging and other mechanisms that allow the company to implement controls over how data is used and accessed.
- To what extent do minimum necessary or data minimization requirements apply? What personal information is the minimum necessary at any given point in the process (e.g., to deploy the product/solution and achieve its primary purpose and for any secondary use activities)?
- What marketing initiatives is the business planning that may need additional review?

Phase 3: Product Maintenance

- If any changes will be made to the product or service, reconsider each of the questions discussed under *Phase 1: Product development* above.
- Are there any new or enhanced risks or vulnerabilities to personal information?
- What proactive steps can a company take to limit the likelihood that privacy violations will occur?

- If there is support offered, what are the policies and processes related to access to customer data or health information by support personnel?

- What plan does the company have to address any privacy or security concerns?

- How often should privacy impact and risk assessments be conducted?

Similar considerations apply to the review of new functionalities, new use cases, or different ways to utilize data that do not necessarily involve the creation of a "product" or "service" but that nonetheless involve collecting, using or disclosing personal information. Engagement with customers, vendors or third parties as part of joint ventures, initiatives or collaborations merits similar review. Each instance may require a modified or abbreviated approach compared to the one described above, and the privacy function may find it useful to establish question lists or checklists for different kinds of review.

For novel or emerging use cases and technologies, such as mixed reality or artificial intelligence, the privacy function may benefit from thinking about privacy by first identifying the types of input and output data involved and then considering the following five foundational activities associated with each type of data:

1. Data creation or collection (including metadata or deidentified information).

2. Data storage.

3. Data access.

4. Data use.

5. Data sharing or redistribution.

There may be different legal or contractual expectations for each such activity and the requirements may differ depending on the type of data. For instance, considerations for publicly available data may differ from those for PHI.

Depending on the size and business model of the organization, the privacy function may see numerous product counseling requests or use case questions. To respond efficiently and effectively, consider whether it may be beneficial to leverage forms or input tools to collect responses to some of these questions for more efficient review. In addition, the privacy function may be consulted at a point in time based on certain assumptions about the product offering and such assumptions may subsequently change. As such, it may be helpful to put in writing information provided about the product or functionality, privacy counsel recommendations, and circumstances in which business stakeholders should re-engage the privacy function to ensure sound review.

If the privacy function is not solely tasked with product counseling — e.g., if product counsel consults with the privacy function as needed — it may be efficient to create resources that colleagues can leverage for initial review.

E. Privacy operations

A privacy function performs a range of day-to-day operational activities to support compliance with applicable privacy laws, as set out below.

1. Support individual privacy rights

Under HIPAA, GDPR, TCPA and other laws, individuals have certain rights with respect to their information. Given the uptick in large scale, highly visible data breaches and contin-

ued global digitization, individuals are also becoming more aware of and protective over their information and privacy. Research also shows that individuals are becoming more selective in the types of information they are willing to share and the manner in which it is shared.129

A privacy function should be responsible for understanding the universe of individual rights that apply to each category of personal information and the industry and societal dynamics that inform how individuals may view or exercise their rights. Such rights include, for example:

- Right to access[130] or data portability[131] — the right for individuals to access and receive a copy of their personal data and other supplementary information. This is commonly referred to as a data subject access request or "DSAR". Data portability also allows individuals to obtain and reuse their personal data for their own purposes across different services.

- Right to amendment[132] or rectification[133] — the right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

- Right to accounting of disclosures (or "right to know")[134] — the right for individuals to request a list of certain types of disclosures made by the organization.

- Right to request restriction of uses, disclosures[135] and processing[136] — the right for individuals to request the restriction or suppression of their personal data.

- Right to request confidential communications[137] — the right for individuals to request that the organization communicate with them via reasonable alternative means.

- Right to object[138] — the right for individuals to object to the processing of their personal data in certain circumstances (e.g., the right to stop their data being used for direct marketing).

- Right to opt out[139] — the right of the individual to opt out of certain uses or disclosures of their information or certain communications.

- Right to opt in — the right of the individual to be free of certain uses or disclosures of their information or certain communications unless the individual opts in.[140]

- Right to request deletion or to be forgotten[141] — the right for individuals' personal data to be erased.

- Right to withdraw consent[142] — the right for individuals to withdraw their consent for the processing of their personal data at any time.

- Right to lodge a complaint with a supervisory authority[143] — the right for EU individuals to lodge a complaint with a supervisory authority.

A privacy function will typically be responsible for understanding and managing operationally how the company abides by such rights. Key issues to consider include:

- What is the specific scope of information that is subject to each right? (E.g., the right of access under HIPAA applies only to PHI in a designated record set and not all PHI about the individual.)

- Relatedly, are there any exceptions to any of the individual rights? (E.g., where the request is unfounded or excessive, or where the information is subject to legal privilege).

- Within what timeframe must a company respond to each request?

As a practical matter, a privacy function should: (a) develop template request forms, procedures and checklists to support compliance with requirements regarding individual rights and (b) maintain records of responses to individuals' requests (including the basis for any denial of such request) for the requisite period.

In addition to responding to individuals' requests to exercise their rights under applicable privacy laws, a company may from time to time receive inquiries or complaints from individuals with respect to a company's privacy or security practices. A privacy function should work together with other stakeholders to investigate and respond to such inquiries and complaints to resolve issues and mitigate risk as appropriate.

The status of an organization under applicable privacy laws will inform how it must support compliance with individual privacy rights. For example, a covered entity under HIPAA is primarily responsible for complying with an individual's right to access PHI maintained in a designated record set,[144] restrict who can access the individual's records, restrict confidential communications, amend their health information if it is inaccurate or incomplete, and obtain an accounting of disclosures of their PHI for purposes other than treatment, payment or healthcare operations.[145] However, business associates may also have compliance obligations if the covered entity has delegated a function to the business associate or if a covered entity requires information from the business associate to meet the covered entity's obligation. As an example, if an individual requests an accounting of disclosures from a covered entity, the covered entity may require the business associate to provide the business associate's accounting of disclosures, which the covered entity can then incorporate into its overall accounting of disclosures.

Moreover, in 2019, OCR introduced the HIPAA Right of Access Initiative to ensure that individuals have timely access to health records at a reasonable cost and, as of the date of this publication, has entered into eighteen settlements with covered entities for failure to respond to an individual in a timely manner.[146] Under HIPAA's right of access, covered entities must respond to individuals no later than 30 days from request in the form and format requested by the individual, if readily producible.[147] Business associates may maintain designated record sets on behalf of covered entities and may need to respond to the covered entity in a timely manner for the covered entity to meet its response timeline. Accordingly, coordination by a covered entity with its business associates is vital for its response to individuals exercising their rights under HIPAA. Covered entities and business associates should, at the onset of their relationship, agree on processes relating to individual rights. For example, if feasible, both organizations can establish an electronic mechanism, such as a designated email address or portal, between the parties to receive and respond to requests related to individual rights.

2. Employee privacy

A privacy function should provide ongoing advice on how the company will protect the privacy of employees' personal information. This advice may include recommendations on how employees' personal information (e.g., personnel file information, health data, financial information or demographic information) may be used, collected and shared. It may also address how a company must maintain sensitive categories of employee data (e.g., the Americans with Disabilities Act's requirement that employers maintain certain medical

information of employees separate from general personnel files). When a company seeks to launch new initiatives involving the collection of employee data, such as return-to-work COVID-19 testing, the privacy function should assess whether the GDPR or federal or state privacy laws require consent to or notice of the data collection or restrict the purposes for which the employee data may be used. In addition, the privacy function should advise on the development and implementation of the company's policies on matters of workplace surveillance, such as drug testing, the monitoring of employees' usage of company-provided computers, telephones, email, the internet and video surveillance.

When a company seeks to launch new initiatives involving the collection of employee data, such as return-to-work COVID-19 testing, the privacy function should assess whether the GDPR or federal or state privacy laws require consent to or notice of the data collection or restrict the purposes for which the employee data may be used.

3. Privacy training

Training a company's business and other stakeholders regarding the privacy laws that apply to a company is not only a best practice but is also a specific requirement under certain laws (such as the HIPAA Security Rule[148]). Effective training places these requirements and obligations into the context of a company's own operations, personnel and business processes.

At a minimum, "general" privacy training should be provided on an annual basis and should cover the privacy laws that apply to the company. Ideally, the general privacy training will incorporate the requirements of disparate privacy laws into one cohesive training rather than separate trainings for each applicable privacy law (e.g., separate trainings for GDPR and HIPAA). The annual, general privacy training is intended to promote general privacy awareness and instruct workforce members regarding where to find additional resources and how to ask questions. It should include a brief description of the privacy principles around which these laws are organized and emphasize only those specifics that are broadly important to the company and its workforce as a whole. This general training should be supplemented by more specific team- or role-based trainings that go in-depth in specific areas that are most relevant to that team or role.

Beyond just training about legal and company expectations, consider whether discussing the company's views related to privacy, compliance and trust may be effective in promoting a culture of privacy. In perpetuating this culture, it may be worthwhile to have internal, privacy-specific reporting mechanisms to make the privacy function aware of potential privacy issues. Whether an organization uses privacy-specific reporting or leverages broader company reporting tools for privacy purposes, ensure that information about how to contact the privacy function to report issues or incidents is a part of all training. By the end of all training, attendees should know whom to call if they encounter a privacy-related issue or potential privacy incidents.

The privacy function may find that some forms of training are more effective than others. Because the ultimate goal is not to disseminate the information but to ensure that it is understood and utilized by the organization, consider whether creative or experimental forms of training may garner better reception. While these should not

serve as a replacement of traditional privacy trainings, the privacy function could look to supplement its standard training with the following components:

- Live privacy exercises (similar to tabletop security incident exercises) where workforce members are asked to spot privacy hazards in a physical setting (e.g., open folders displaying patient files inside, passwords on notes taped to computer monitors, etc.).

- Interactive activities, such as role-play scenarios, quizzes or games that encourage application of privacy training materials.

- Recorded videos or digital simulations showcasing appropriate responses to privacy scenarios.

Note that training or supplemental activities can also be outsourced to other functions or vendors to preserve the limited time of the privacy function.

4. Regulatory and litigation response

From time to time, a company may receive inquiries or communications from regulators such as OCR, EU data protection authorities, state attorneys general, and other governmental authorities, customers or vendors, and/or individuals or representative groups (acting on behalf of affected individuals, including through class actions). In addition, a company may from time to time be involved in litigation that relates to a company's collection, retention, use and disclosure of data. A privacy function should coordinate with the company's litigation team to assess and respond to such inquiries, claims, communications and matters.

The privacy function will often be the first point of contact for individuals and regulators who may have a concern, complaint or other communication in relation to a company's privacy practices. The privacy function should ensure that consistent and clear communications are issued in response to inquiries.

5. Support M&A activities

As a company explores and pursues mergers, acquisitions and other transactions, a privacy function should support the deal team (including in-house and outside legal counsel) by conducting or supporting privacy due diligence in connection with the transactions. Key pre-closing responsibilities include:

- Identifying the scope of appropriate privacy diligence and key focus areas and potential areas of concern.

- Reviewing responses to diligence requests.

- Evaluating preliminary and final diligence findings.

- Attending debriefing calls with outside counsel regarding diligence findings.

- Advising company leadership and other stakeholders on privacy risks and remediation and integration costs, privacy impacts on the value of transaction, and other considerations such as customer, patient or public relations risks, based on diligence findings.

Post closing, a privacy function supports integration in the following ways:

- Address and remediate diligence findings.

- Triage diligence findings, such as by identifying any diligence findings for which a longer-term remediation plan is appropriate.

- Integrate the privacy functions of the post-transaction company.

- Determine and address any impact of the transaction on the legal, organizational, or operational dimensions of the post-transaction company (e.g., due to a change in the status of the company under HIPAA or the GDPR, whether there are any new or different restrictions on how the company may use and disclose personal information).

- Provide any new or additional privacy training.

Finally, a privacy function may be called upon to review draft filings (such as annual or quarterly reports) with the U.S. Securities and Exchange Commission and similar filings in other countries. Working with outside counsel as appropriate, a privacy function may review such filings to confirm that they accurately describe the company's business, the legal and regulatory requirements that apply to the company with respect to privacy, and the extent and nature of privacy risks to the company's business based on legal and regulatory requirements, enforcement trends and the broader industry landscape. Key sections of focus may include the "Business" and "Risk Factors" sections of SEC filings.

6. Engage with company leadership

Stemming from the COVID-19 pandemic, now more than ever the health industry has accelerated its pace in technology adoption and has begun taking a data-driven approach to solving complex problems and identifying new avenues for growth. The privacy function can play a strong role in helping company leadership think about business strategy by demystifying the rules associated with different kinds of data. The privacy function may, for example, advise company leadership on the following issues:

- Significant new privacy developments that impact the business and require a decision by or guidance from company leadership.

- The occurrence of and response to breaches or other privacy incidents.

- Updates regarding notable regulatory actions or litigation involving the company or the company's competitors.

In this capacity, a privacy function should also educate company leadership and obtain company buy-in on the importance of privacy. Because administrative functions, such as legal, privacy and compliance are typically viewed as cost centers, there may be leadership hesitancy to invest in or expand the privacy function more than necessary. To address this, it can be valuable to present both the current work/value of the privacy function as well as describe the role of privacy in supporting potential strategic or growth opportunities for the organization. Given the importance of data to healthcare organizations and the regulatory complexity associated with the use of health data, a robust privacy function is an important stakeholder in establishing and implementing a company's data strategy.

7. Privacy outreach and awareness-building

Privacy can be a market differentiator for healthcare companies, particularly as the political landscape in Europe becomes more protective of individual rights vis-a-vis privacy and as more states in the U.S.

enact more restrictive privacy legislation. A privacy function can play an important role in shaping the company's philosophy on privacy and communicating this philosophy and the company's approach toward privacy to patients, members, customers, vendors, business collaborators and the public at large. A company's communication strategy may include publications through journals, white papers and presentations at industry conferences (such as IAPP, Privacy & Security Academy AHLA), and developing relationships and engaging with key opinion leaders in the industry. Moreover, the privacy function, either through the use of its executives or through industry groups, can help influence policy on behalf of the organization.

F. Privacy risk assessments

An organization may be subject to privacy laws that require it to conduct initial and periodic assessments of its data processing activities. The organization's privacy function should lead efforts to assess privacy risks and to document such assessments. The privacy function should also lead the remediation, as appropriate, of privacy risks identified. Privacy risk assessments may take a range of different formats, but at core, involve assessing the compliance of a product, service, or activity with legal requirements, contractual obligations and external privacy commitments (e.g. website privacy notice).

The following discussion reviews three types of privacy risk assessments: (1) privacy impact assessments, which are a tool recommended by the FTC and other privacy regulators, (2) Record of Processing under GDPR, and (3) Data Protection Impact Assessments under GDPR. While RoP are not strictly a privacy risk assessment, they are a foundational activity in support of privacy risk assessments and are a tool used to determine the activities for which a DPIA would be appropriate.

1. Privacy Impact Assessments

A privacy impact assessment is an assessment by a privacy function of whether a product, service or activity complies with applicable privacy requirements. A PIA can take many different forms. At its most basic, it could ask a series of simple questions to product owners asking them to describe the new product or service, with a space at the bottom for a member of the privacy function to fill in the analysis of the product with respect to privacy laws. But it can also be a more extensive analysis of the privacy risks to individuals with respect to a product or service, along with mitigations to reduce the risk.

One effective PIA tool is to write a narrative of the data processing activities for a product or service, from the moment the data is created or received, to all the systems where the data is stored, who has access to it and how it is used (i.e. a full and complete description of the data processing). While Excel spreadsheets, data flow diagrams and other detailed representations of data processing can be a useful tool, they also may contain a level of detail and complexity that can be overwhelming. The narrative can distill data processing activities to their essence, with cross-references to other documents that contain further details, and can be a foundational document with which to assess privacy risks at a deeper level. This narrative can also help form the basis for record of processing, DPIAs and other privacy assessments.

2. GDPR record of processing activities

A company is required under GDPR to complete and keep an up-to-date record of processing activities. This work can be used to: (1) determine whether a company has the appropriate agreements in place, (2) catalogue the various categories of data a company receives or generates, its data sources, the purposes

for which data is used and disclosed, and to whom data is disclosed, (3) assess applicable laws, (4) assess a company's role with respect to various data sets (e.g., data processor or data controller), (5) confirm appropriate data pathways or bases for processing data, (6) determine whether the company has implemented necessary safeguards to ensure appropriate use, including any necessary firewalls, access controls, authentication mechanisms, compartmentalization or other mechanisms to support role-based access restrictions, (7) determine any needed contract updates and (8) provide overall compliance oversight.

The privacy function should manage the completion and maintenance of the record of processing and may provide a template for documentation of the same. Two templates may be appropriate where the company is, in various contexts, either a controller or a processor. A template record of processing may be as simple as a spreadsheet that is designed to capture and memorialize the below categories of information.

As to controllers:

- Categories of individuals.
- Categories of personal data.
- Purposes of processing.
- Categories of recipients.
- Other countries or international organizations to which personal data is transferred.
- Safeguards for exceptional transfers of personal data to other countries or international organizations.
- Retention schedule.
- General description of technical and organizational security measures.
- Applicable privacy notices (Article 6 lawful basis for processing personal data, Article 9 condition for processing special category data, the source of the personal data).
- Location of personal data.
- Whether a DPIA is required.
- Whether a personal data breach has occurred.

As to processors:

- Name and contact details of the controller's representative.
- Categories of processing.
- Other countries or international organizations to which personal data is transferred.
- Safeguards for exceptional transfers of personal data to other countries or international organizations.
- General description of technical and organizational security measures.

3. GDPR data protection impact assessments

A DPIA is a requirement under the GDPR for certain "high-risk" processing activities. While DPIAs consider compliance risks (i.e., legal risks to the enterprise), they also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage.

The privacy function should manage the DPIA process centrally. In practice, this should involve:

- *Step 1 – Identifying when a DPIA is required:* EU guidance confirms that certain activities (i.e., certain risk factors/criterions) would require a DPIA under the GDPR. Privacy should identify whether a new project or processing activity involves the following[149]:
  - Evaluation or scoring (e.g., building marketing profiles based on website usage).
  - Automated decision-making with significant effects (e.g., where any processing could lead to discrimination).
  - Systematic monitoring (e.g., if a new IT monitoring system is deployed to monitor employee emails).
  - Processing of sensitive data or data of a highly personal nature (e.g., the analysis of health or genetic information).
  - Processing on a large scale (e.g., a processing activity involving a large number of individuals or a processing activity involving a large volume of data or wide range of different data items being processed, such as big data analytics).
  - Processing of data concerning vulnerable data subjects (e.g., offering services to mentally incapacitated individuals).
  - Innovative technological or organizational solutions (e.g., using AI or other innovative technology).
  - Combining, comparing or matching data from multiple sources.
- *Step 2 — Completion of the DPIA template:* The privacy function should develop a DPIA template, to be used to describe how and why personal information will be used in connection with the specific project.
- *Step 3 — Consultation:* The privacy function should consult all relevant internal stakeholders, in particular, anyone with responsibility for information security and the lead of the project. The privacy function should also consider whether consultation with third parties is necessary. For example, if a data processor (e.g., IT supplier) is used, then it may be necessary to ask that third party for information and assistance.
- *Step 4 — Identification of risk:* To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. In particular, when identifying risks, the privacy function should look at whether the processing of personal information in the project could contribute to:
  - Inability to exercise rights (including but not limited to privacy rights).
  - Inability to access services or opportunities.
  - Loss of control over the use of personal data.
  - Discrimination.
  - Identity theft or fraud.
  - Financial loss.
  - Reputational damage for an individual.
  - Physical harm.

- Loss of confidentiality.
- Reidentification of pseudonymized data.
- Any other significant economic or social disadvantage.

- *Step 5 — Risk Mitigation:* A DPIA does not have to indicate that all risks have been eliminated. But it should help document them and assess whether or not any remaining risks are justified. It should suggest mitigation steps, for example, introducing additional security measures such as a higher level of encryption, making changes to privacy notices or anonymizing data.

- *Step 6 — Sign off:* Once the DPIA has been completed, the privacy function should sign off on the document and retain a record. The privacy function should help integrate the outcomes of the DPIA into the project plans and continue to consult, as needed, on the implementation of the project plans.

G. Coordination with security function

In most organizations, the privacy and security functions have a symbiotic relationship. A privacy function should support the development, implementation, maintenance and enforcement of an organization's data security program. For example, although HIPAA requires the designation of a security official who is responsible for the development and implementation of policies and procedures required by the HIPAA Security Rule, in practice, the privacy function and security function often work together closely in this regard.

The privacy function may often assist or collaborate with the security function on such matters as security program scoping and design (particularly with respect to implementing the privacy requirements of applicable data security or protection laws), security policy documentation, ensuring policies are reviewed and security risk analyses are conducted with appropriate frequency, security incident investigation, workforce member training and data mapping. Such collaboration is often beneficial to the privacy function, the security function and the organization as a whole because the privacy function's legal and compliance skill sets complement the security function's technical skill set. Below we describe areas of collaboration in more detail.

1. Incident response

Privacy incidents, security incidents, and potential or actual breaches of sensitive information often entail examination of related issues of privacy and security compliance. For example, the hack of an email account may require technical investigation by the security function and consideration by the privacy function as to whether an unauthorized use or disclosure of sensitive information occurred in light of organizational policies and applicable law. The privacy and security functions typically cooperate in such investigations and may comprise standing members of a broader, formalized privacy or security incident investigation committee. Almost all privacy incidents relating to health information stored electronically are also security incidents.

A privacy function should be involved in responding to privacy and security incidents in a fast, planned and coordinated manner. This will typically include, as to privacy incidents, a primary investigatory and response role and, as to security incidents, a supporting role managing a concerted investigation with IT security colleagues. For all incidents, the

privacy function may assess breach notification obligations and coordinate breach notifications where required by applicable law.

For an effective incident response program, the privacy and security functions can jointly develop policies and procedures for identifying and responding to incidents such that at the time of an incident, the role and responsibility of each function are clear. To achieve this, some organizations engage in "tabletop" exercises in which they respond to a fictional incident in accordance with their papered processes and refine the process based on the outcomes of the exercise.

2. Third-party audits and certifications

The privacy and security functions need to routinely collaborate as part of third-party audits and certifications, such as ISO, HITRUST or SOC. Preparation for these audits occurs long before the audit date through gap analyses and internal audits. This preparation period is typically spearheaded by the security function, but some organizations may take a co-lead approach where both functions jointly guide the organization through this phase. Upon identification of gaps, the privacy function and security function (with support from other stakeholders) typically work to fill these gaps.

The criteria and process for each type of audit differ, but an audit typically involves three main stages: (1) advance document review by auditors, (2) the in-person audit, including interviews with relevant stakeholders, and (3) discussion of and response to audit results. For the first stage, both privacy and security functions need to work collaboratively to produce documents requested by the auditor. Audits may ask for policies that involve both the privacy and security function. For the second stage, both the privacy and security functions may be interviewed, and the auditors may also interview other internal stakeholders who may need to be prepared in advance for the audit. Lastly, auditors will typically go over results with relevant stakeholders who in turn assess how best to remedy any deficiencies. This can be a fast-paced process and having a good working relationship between the privacy and security function can be instrumental to a successful audit.

After audits, as part of contract negotiations or as part of routine diligence, customers or other third parties may ask for reports or certifications from these audits or for organizations to complete security or privacy questionnaires or assessments. In some organizations, these may be completed by the security function with support from the privacy function.

3. Data governance

Having an established strategy and protocols for data governance can be a true differentiator for organizations. NIST defines data governance as a set of processes that ensures important data assets are formally managed throughout the enterprise.[150] Data governance can include development of data use and access policies, adopting technology solutions to implement such policies, data security, data mapping, data cataloging and data quality review. A data governance function may be set up as a separate function within a company, but privacy and security functions are important stakeholders in supporting a data governance function. As an example, for data access decisions, the privacy function may establish who and under what circumstances may access a particular data set, while the security function would ensure that appropriate technical controls are in place to set appropriate limits on access to the data set.

4. Security program scoping

As between the privacy function and the security function, the privacy function will have greater awareness of applicable privacy laws. Such laws may not only contain security requirements (e.g., HIPAA) but also may contain privacy requirements that must be built into or otherwise solved for by the security program. Examples of privacy requirements that may be incorporated into a security program include:

- CCPA provides consumers with certain rights related to their personal information, which rights may require the inclusion of certain data tagging and other technical functions.

- GDPR includes robust data deletion rights and the implementation of such rights may require data tagging.

A privacy function can help orient the security function regarding these and other requirements that should be considered in the development and maintenance of the security program.

Also, to maintain consistency across the written privacy and security compliance programs, the privacy function may participate at a high level in the development of the security program. Such participation may help ensure that the written privacy and security policies and procedures are consistent with and appropriately dovetail with and cross-reference each other.

5. HIPAA security risk analysis

A privacy function also plays an important role in advising on the legal requirements under HIPAA for conducting a "security risk analysis." This is a key compliance activity under HIPAA. In a security risk analysis, HIPAA-regulated entities assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. The analysis should result in risk ratings for all threat and vulnerability combinations identified across the enterprise. The entity should identify mitigation strategies to reduce identified risks to reasonable and appropriate levels and determine whether to accept any identified risks based on its risk tolerances.

> ***To maintain consistency across the written privacy and security compliance programs, the privacy function may participate at a high level in the development of the security program.***

HIPAA requires that the analysis be regularly updated. Organizations frequently select a typical cadence for such updates (e.g., annually). A privacy function may "check in" with the security officer to ensure such updates are occurring and help shepherd and support the process from project inception to completion. In addition, a security risk analysis should be updated to reflect, if needed, new product or service offerings, corporate transactions or other material organizational changes that may not be evident to the security function. The privacy function could help ensure the security function is made aware of such changes that may precipitate a need to update the security risk analysis.

A HIPAA Security Rule compliance gap assessment is not specifically required by HIPAA but provides a helpful foundation for a company to complete its HIPAA security risk analysis and is frequently completed as part of the HIPAA security risk analysis process. The HIPAA Security Rule is grouped into three categories of controls, which

are called safeguards: (1) administrative safeguards; (2) physical safeguards; and (3) technical safeguards. The Rule also includes "implementation specifications" — or specific requirements — for satisfying the security standards. A HIPAA Security Rule compliance gap assessment identifies the security standards and the implementation specifications under each security standard, resulting in the identification of any gaps and forming the foundation of a remediation plan.

H. Coordination with other regulatory and compliance functions

An effective healthcare privacy function should involve regular coordination with other compliance personnel and regulatory counsel.

With regard to compliance, most organizations in the health industry have a compliance program in place. Organizations such as hospitals, physician practices, home health agencies, hospice, nursing facilities, and durable medical equipment and pharmaceutical manufacturers generally have a compliance function that stems from guidelines set forth by the Office of Inspector General within HHS to prevent health fraud and abuse. Other entities may have compliance programs stemming from other applicable laws or guidelines such as to prevent anti-corruption and anti-bribery compliance, while some may establish general compliance programs to ensure that internal processes align with legal and regulatory requirements. As part of efficient internal processes, the privacy function may benefit from teaming up with other compliance personnel in the following areas:

- Establishing and disseminating policies and procedures.
- Internal training.
- Reporting of noncompliance with policies and procedures.
- Appropriate remediation for noncompliance.

In certain instances, the privacy function may be integral to regulatory and compliance efforts. Below are three examples.

1. Information Blocking

The privacy function should support an organization's compliance with information blocking rules and the implementation of processes for the appropriate exchange or transition of health information. Information blocking is defined as any practice that is likely to interfere with access, exchange, or use of electronic health information[151] that an organization knowingly engages in or, in the case of healthcare providers, is unreasonable.[152] These rules apply to healthcare providers, health information networks/health information exchanges and developers of certified IT (namely, EHR systems and health IT modules), which are collectively categorized as "actors" within the regulations. Exceptions to the information blocking regulations fall into two categories: (i) those that apply when an actor is not fulfilling a request for access, exchange or use of EHI, and (ii) those that specify the procedure for fulfilling such requests. To avoid risk of information blocking, an actor must either provide access to all EHI that is requested or satisfy the requirements for an exception.[153]

While each organization's approach to compliance may differ, the following should be key for an effective approach to information blocking compliance:

a. Multi-stakeholder engagement: Given the expansiveness of the information blocking rules, organizations will need

to engage various departments and stakeholders for information blocking rule compliance, including: legal, privacy, compliance, security, finance, product development and business strategy. Some organizations establish a working group with members from each of these departments to spearhead information blocking compliance efforts.

b. Assessment of impacted health information and processes: Organizations will need to identify the types of information and practices that may be subject to information blocking rule by doing the following:

   - Identify the types of information held by the organization that meet the definition of EHI.
   - Assess whether any products or services offered by the organization contain EHI. Additionally, assess which types of EHI individuals may routinely request and consider prioritizing compliance efforts for these types of EHI.
   - Identify internal materials or assets that meet the definition of an interoperability element (i.e., materials or assets that access or use EHI).
   - Review how requests for EHI or interoperability elements are received and processed, including timing of response.
   - Assess whether any examples provided by ONC as information blocking reflect current practices of the organization.

c. Assess agreements and establish policies: Activities for which a privacy function, in coordination with compliance and regulatory counsel, should look to play a key role include reviewing BAAs and other agreements to ensure that provisions within the documents do not constitute an interference to the access, use or exchange of EHI; establishing policies and procedures for each exception under the information blocking rules and for monitoring and responding to requests for EHI or interoperability elements; and establishing a process to review and a provide counsel on whether certain activities constitute information blocking.

2. Required Exchange of Health Information

Covered entities have always been required to adopt and comply with certain standards for the electronic exchange of health information. For instance, HIPAA, as part of the Administration Simplification Rules, mandates the use of various standard transactions for purposes such as submitting healthcare claims, eligibility verification and claims status. The privacy function may be tasked with assisting internal stakeholders with compliance with these requirements. Moreover, as part of national interoperability efforts, organizations are being expected to enable the efficient exchange and use of clinical and administrative health information.

The ONC and CMS Final Rules newly require the health industry to adopt, among other things, the Fast Healthcare Interoperability Resources standard for this purpose. For example, certain types of health plans must implement and maintain a FHIR-based application programming interface to make available claims data, encounter data, clinical data, and formulary or covered drug information to third-party applications at the direction of the patient. In addition, EHRs must soon allow for providers to export EHI using the FHIR standard. The privacy function

should remain aware of these data sharing requirements and implications for patient privacy. For instance, prior to responding to a patient request to share information with a third-party application, providers and payers may be expected to educate patients about potential privacy risks.

3. Human subject protection compliance

An organization that conducts research involving human subjects, or releases information or biospecimens for use in research by third parties must also identify and comply with applicable requirements and restrictions under human subject protection laws. As described above, such laws may include state medical experimentation and human subject protection laws, and federal laws and regulations that regulate federally funded or supported human subjects research, or research that is intended to generate data for submission to the FDA. Due to the overlap in privacy and human subject protection laws, a privacy function should be involved in or otherwise consulted during the design and implementation of human subject research or release of information or biospecimens to third parties for research.

While informed consent designed to educate an individual about what participating in a research study entails and the potential risks and benefits of such participation is legally distinct from a consent or authorization that documents permission to use or disclose an individual's personal information or PHI, there are parallels between the two kinds of permissions. First, the factors that inform when either form of permission is required are closely related. For an IRB or privacy board to waive or alter the requirement to obtain a HIPAA authorization, it must determine, among other things, that the proposed use or disclosure of PHI presents "no more than a minimal risk to the privacy of individuals" and that the research "could not practicably be conducted without the waiver or alteration…." Similarly, for an IRB to waive or alter the requirement to obtain informed consent under the Common Rule or FDA GCP regulations, it must determine that the research presents "no more than minimal risk to the subjects" and that the research "could not practicably be carried out without the requested waiver or alteration." In addition, the content of an informed consent required for human subject protection purposes and a consent or authorization for privacy purposes generally seek to achieve the same purpose — to provide certain information regarding what will happen to the individual or the individual's personal information or PHI, and the potential risks to the individual by providing the permission requested.

As a practical matter, the intersection of privacy and human subject protection laws and regulations materializes in the following common areas: (i) determining when an activity constitutes research (which may be solely by virtue of the research use of identifiable private information); (ii) determining privacy pathways for the conduct of "preparatory to research" activities such as subject screening and recruitment; (iii) determining when informed consent and privacy consents/authorizations are required and when IRB or privacy board waiver is appropriate; (iii) preparing study protocols, information sheets, IRB forms, and related study materials; (iv) communicating with IRBs and regulators; (v) reviewing proposed publications to determine appropriate deidentification and anonymization of study results and study data; and (vi) supporting incident response and IRB, sponsor, and regulator notifications and management in the event of inappropriate uses or disclosures of subjects' personal information or PHI in connection with research.

> ***Privacy involvement helps confirm that a company collects, retains, uses and discloses personal information, redacted information in accordance with privacy laws, consent forms and agreements.***

Accordingly, an organization should carefully allocate responsibility between, and coordinate the operation of, its privacy function and research compliance function for determining the applicability of human subject protection laws, synthesizing overlapping requirements, and harmonizing inconsistent requirements. For example, where IRB review is not required for a particular research study that falls into an exemption category under the Common Rule, an organization may nonetheless seek an IRB or privacy board waiver of HIPAA authorization for the use or disclosure of any PHI in connection with such exempt research. Particularly where an organization's research compliance function is distinct from its privacy compliance function, it will be important to implement policies, procedures, training and other safeguards to help ensure that these overlapping but distinct regulatory regimes are appropriately addressed.

It may be helpful for a privacy function's responsibilities to include supporting the development of documentation relating to a company's research activities. Privacy involvement helps confirm that a company collects, retains, uses and discloses personal information, redacted information (i.e., deidentified, pseudonymized, and anonymized data sets and limited data sets) in accordance with privacy laws, consent forms and agreements. Key privacy documentation and responsibilities may include:

- Determining when any standing IRB protocols can help streamline a company's research activities, particularly those that are recurring and minimal risk (such as internal use of personal information for research).
- Helping to draft IRB protocols, informed consent forms, and HIPAA authorizations and privacy consents used for research purposes; advise on any necessary amendments as changes to research arise.
- Helping to draft emails and other communications for use in subject recruitment and ensure that such activities comply with applicable privacy laws, underlying consents and agreements.
- Communicating with IRBs as appropriate, such as to obtain the IRB's preliminary thoughts on proposed research and whether a standing protocol would be appropriate.
- Reviewing proposed publications to ensure proper any subject data is appropriately deidentified or anonymized (except where publication of personal information is specifically permitted under applicable subject enrollment materials and IRB protocols, such as for subjects with particularly rare genetic conditions or studies that require the publication of images of a subject's face).

IV. Recommendations

In the ecosystem of healthcare industry and adjacent companies, privacy is and will increasingly be a competitive differentiator. Privacy functions that successfully navigate the ostensibly competing tensions of compliance, transparency and innovation will distinguish their organizations in the marketplace by producing innovative new products, solutions and insights gleaned from

rich repositories of usable data by promoting consumer trust and brand-loyalty through transparent privacy practices, and by adapting to swiftly evolving regulatory landscapes. Such success does not occur by accident. It requires a skilled privacy function that is highly knowledgeable about the present and evolving regulatory landscape and that carefully plans, builds, implements and manages a compliant privacy program that is flexible and scalable, intersects appropriately with security, product design and other relevant functions, and maximizes data utility to drive future innovation and growth.

Drawing on the pillars discussed above and on our personal experiences as in-house and external privacy specialists, we have distilled a number of recommendations for our colleagues in healthcare privacy functions. The following recommendations are not intended as a "one-size-fits-all checklist" but rather as a "menu" of items to consider for implementation.

A. Build sustainable processes and resources

- Consider developing self-help guidance for the business teams and other groups that require privacy support.

- If there is an influx of questions in one area, consider bringing the knowledge to the requesters through specific training or by leveraging "privacy champions" who are trained by the privacy function to respond to routine questions.

- Evaluate whether a privacy repository or webpage (e.g., a SharePoint site) makes sense for your organization.

- Keep metrics on what the privacy function handles. This comes in handy when asking for additional headcount and for general team planning.

> ***If there is an influx of questions in one area, consider bringing the knowledge to the requesters through specific training or by leveraging "privacy champions" who are trained by the privacy function to respond to routine questions.***

B. Expand and maintain the currency of your privacy knowledge base

- Keep abreast of the regulations relevant to your function and organization. We have provided citations throughout this paper to assist in that respect.

- Subscribe to regulatory and industry email listservs. We recommend, in particular, listservs from HHS OCR privacy and security,[154] IAPP,[155] outside counsel, Cybersecurity and Privacy Law360 (currently a paid subscription), Practical Law (currently a paid subscription) and Healthcare Info Security.[156]

- Follow the social media (e.g., Twitter) accounts of regulators and privacy subject matter experts, such as the UK Information Commissioner's Office, EU Data Protection Authorities, @HealthPriv, Chris Hoofnagle (@hoofnagle), Lucia Savage (@savagelucia), Paul Schwartz (@paulmschwartz), and Daniel Solove (@DanielSolove).Review guidance from influential EU bodies, such as the European Data Protection Board[157] and European Data Protection Supervisor's website.[158]

- Attend privacy conferences and look for speaking or presentation opportunities. Such conferences include IAPP, Privacy and Security Forum, HIMSS and AHLA.

- Learn enough about security to speak the language, know what is going on, and spot issues. We find Krebs on Security[159] to be a helpful resource.

> ***To the extent the organization engages in research or research-related activities, the privacy function should engage with the research compliance function to ensure appropriate consents are obtained and that data is used or disclosed only for permitted purposes.***

C. Engage with other relevant functions

- Know and have an ongoing working relationship with personnel in the product development organization. Seek to insert the privacy function at key decision or product/service development points. Consultation with privacy on the front end can save work and time on the back end.

- Engage with the security function as discussed in this paper. Perhaps schedule at least quarterly general check-ins and coordinate privacy and security program reviews at least annually. Ensure the security function understands privacy obligations and develops mutual objectives with respect to data flows, tagging and data utility.

- Promote consistent use of terminology for data categories and processes across the organization.

- To the extent the organization engages in research or research-related activities, the privacy function should engage with the research compliance function to ensure appropriate consents are obtained and that data is used or disclosed only for permitted purposes. More fundamentally, the privacy function should support the analysis of whether analytics, insights generation or other activities constitute "research" activities, and if they do, determine the research-related compliance requirements that would then attach to the activity.

- Maintain relationships and consult readily with the legal or broader compliance functions.

- Coordinate with the human resources function as appropriate with respect to training (e.g., frequency and content) and workforce member sanctions, roles, access rights, and new hires and terminations.

D. Train (and retrain) workforce members

- Ensure workforce members are appropriately trained regarding privacy compliance. Interface with human resources or the compliance function as required to accomplish this objective.

- Within training presentations, harmonize disparate requirements in a cohesive way to make content readily understandable to non-experts.

- Send weekly or monthly "privacy reminder" emails on rotating, relevant topics.

- Consider in-person privacy training "exercises" (analogous to tabletop security incident exercises) where workforce members are asked to spot privacy hazards in a physical setting (e.g., open folders displaying patient files inside, passwords on notes taped to computer

monitors, etc.). Although probably not a substitute for traditional privacy training programs, such exercises may be creative, fun and engaging additions to passive training events or e-learning modules.

- Ensure workforce members (and consumers and patients) know who to call if they encounter a privacy-related issue or potential privacy incidents.

E. Seek and maintain relationships with other privacy professionals

- Exchange tips and best practices and conduct "gut checks" with trusted privacy colleagues in other organizations.

F. Develop a "data map" for your organization or product or service line

- We have found it valuable to reduce data collection/creation/inputs and subsequent flows, curation, maintenance, and uses and disclosures to a data map for enhancing understanding, compliance and utility.

- It is critical that the security function also participates in the data mapping exercise.

G. Identify external vendors and other support

- Engage strong outside privacy and breach response counsel (or work with in-house counsel if appropriate) with respect to more complex analyses, broader industry perspective and approaches and privacy incident response. With respect to privacy incident response in particular, having an engagement established in advance of an incident is critical to ensure key aspects of incident investigations are conducted at the outset under attorney-client privilege.

- To the extent the organization uses PHI to create deidentified health information, consider the utility of statistical deidentification versus the "safe harbor" approach of deidentification. Identify qualified statistical experts to provide deidentification opinions if that is the preferred deidentification approach.

- Consider whether the organization may benefit from leveraging privacy compliance tools for training, documentation or supporting individual privacy rights.

Engage strong outside privacy and breach response counsel (or work with in-house counsel if appropriate) with respect to more complex analyses, broader industry perspective and approaches and privacy incident response.

H. Maintain and drive a privacy "vision"

- Show leadership what the organization needs to succeed. Demonstrate long-term strategic planning. Rather than presenting privacy as an obstacle, present privacy initiatives as differentiating, enhancing and promoting innovation.

- Given that most privacy functions are considered cost centers, the organization may not be willing to invest heavily in all privacy initiatives instantly. In that regard, focus on addressing the most important privacy initiatives first and consider implementing metrics to track the work the privacy function is performing.

Checklist for healthcare privacy program pillars

The below checklist is designed to be a high-level reference that outlines the key pillars of a healthcare privacy program, as described in more detail in this article.

CONDUCT AND PROVIDE LEGAL ANALYSIS

- ☐ Establish a procedure to identify, analyze and provide guidance on applicable privacy laws as well as laws that intersect with privacy, including marketing and human subject protection laws.
- ☐ Consider appropriate format of written legal analyses in light of operational and business needs (e.g., memoranda, guidelines or checklists).
- ☐ Maintain and centralize written analyses to support institutional knowledge and ease of reference.
- ☐ Monitor legal developments through regulatory and industry email listservs, privacy conferences, and social media.
- ☐ Develop networks and resources among privacy professionals and bar associations.

POLICIES, PROCEDURES AND GUIDELINES

- ☐ Develop internal policies and procedures, including an index or centralized repository for easy navigation.
- ☐ Develop checklists, FAQs and other practical tools to facilitate privacy compliance and ensure that business stakeholders know that these resources are available.
- ☐ Develop external privacy notices and consents.

CONTRACTING

- ☐ Support customer, vendor and other contracting, including advising on when privacy-specific terms or agreements (such as business associate agreements) are required.
- ☐ Develop template privacy-related contracts and provisions and contracting playbooks to support negotiations.
- ☐ Support privacy diligence of vendors and ongoing oversight.

PRODUCT COUNSELING

- ☐ Support privacy by design through all phases of product development, including ongoing evaluation and monitoring.
- ☐ Create a process for efficient review by privacy counsel, including leveraging colleagues and using forms or other tools to collect necessary information.

PRIVACY OPERATIONS

- ☐ Support individual privacy rights, including development of template request forms, procedures and checklists.
- ☐ Advise on protection of employee personal information.
- ☐ Provide training in a manner that promotes meaningful comprehension and culture of privacy.
- ☐ Support regulatory and litigation response.
- ☐ Support M&A activity, including privacy diligence.
- ☐ Engage with company leadership and advise on long-term data strategy.
- ☐ Support privacy outreach and awareness-building.

PRIVACY RISK ASSESSMENTS

- ☐ Conduct privacy impact assessments.
- ☐ Manage GDPR record of processing activities.
- ☐ Manage GDPR data protection impact assessments.

SECURITY COORDINATION

- ☐ Coordinate and collaborate with the security function.
- ☐ Support incident response.
- ☐ Support preparation for third-party audits and certification efforts.
- ☐ Support development of strategy and process for data governance.
- ☐ Support security program scoping.
- ☐ Advise on HIPAA security risk analyses.

COORDINATION WITH OTHER REGULATORY AND COMPLIANCE FUNCTIONS

- ☐ Coordinate and collaborate with regulatory and compliance functions.
- ☐ Support compliance with information blocking rules and standards for the electronic exchange of health information.
- ☐ Support compliance with human subject protection requirements, which include privacy and confidentiality protections for research subjects.

Endnotes

1 When we refer to healthcare companies, we broadly mean organizations that as a component of their business collect, create, receive, maintain, transmit, use, disclose or otherwise process health information. This may include healthcare providers, health plans, healthcare clearinghouses, and adjacent companies or service providers, including IT service providers, data analytics companies and administrative services providers.

2 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

3 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5 §§ 13001–13421, 123 Stat. 226 (2009).

4 45 C.F.R. pts. 160, 162, and 164.

5 *See id.* pt. 160 and subparts A and E of pt. 164.

6 *See id.* pts. 160 and 164, subparts A and C.

7 *See id.* §§ 164.400–414.

8 *See* 45 C.F.R. § 160.103 (definitions of "Individually Identifiable Health Information" and "Protected Health Information"). PHI excludes certain education and employment records held by a person as an employer. See 45 C.F.R. § 160.103 (definition of "Protected Health Information").

9 *See* 45 C.F.R. § 160.103 (definition of "Covered Entity").

10 *See id.* § 160.103 (definition of "Business Associate").

11 *See id.* § 164.530(a)(1)(i).

12 *See id.* § 164.308(a)(2).

13 *See id.* § 164.530(i). HIPAA does not require business associates to maintain written policies and procedures implementing HIPAA's privacy and breach notification standards, but many business associates do as a best practice.

14 *See id.* § 164.316(a).

15 *See id.* § 164.414(a). *See also* U.S. Dep't of Health & Hum. Servs. Off. for C.R., *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Mar. 10, 2021) ("[C]overed entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.").

16 *See* 45 C.F.R. § 164.520.

17 *See id.* § 160.103 (definition of "Electronic Protected Health Information").

18 *See id.* § 164.308(a)(1)(ii)(A).

19 *See id.* § 164.402 (definition of "Breach").

20 *See id.* § 164.402 (definition of "Unsecured Protected Health Information").

21 *See id.* § 164.404.

22 *See id.* § 164.408.

23 *See id.* § 164.406.

24 *See id.* §§ 164.504(e) & 164.504(e).

25 *See id.* § 164.530(b)(1).

26 *See id.* § 160.404. OCR adjusts the penalty ranges periodically for inflation.

27 *See id.* § 160.416.

28 Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881.

29 26 C.F.R. pt. 54; 29 C.F.R. pt. 2590; 45 C.F.R. pts. 144, 146, 148, 160, 164.

30 29 C.F.R. pt. 1635.

31 *See, e.g.*, 29 C.F.R. § 1635.2; 26 C.F.R. § 54.9802-3T(a)(3).

32 42 U.S.C. § 290dd-2.

33 42 C.F.R §§ 2.1–2.67.

34 42 U.S.C. § 290dd-2.

35 42 C.F.R. §§ 2.31–2.35; 42 C.F.R. §§ 2.61–2.67.

36 42 C.F.R. §§ 2.51–2.52.

37 *Id.* § 2.31(a).

38 A "lawful holder" is an individual or entity that has received patient identifying information as the result of a consent compliant with Part 2 or as otherwise permitted under Part 2.

39 42 C.F.R. § 2.11.

40 85 Fed. Reg. 42986, 42995 (July 15, 2020).

41 *Id.* at 42996.

42 The 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).

43 45 C.F.R. § 160.202 (defining "Contrary" in the context of preemption as meaning (1) "A covered entity or business associate would find it impossible to comply with both the State and Federal requirements;" or (2) "The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of [HIPAA]").

44 *Id.* § 160.203.

45 *See, e.g.*, Cal. Civ. Code §§ 56–56.37.

46 18 Vt. Stat. Ann. § 7103.

47 Ala. Code § 22-11A-22 (1975).

48 *See, e.g.*, N.Y. Civ. Rights Law § 79-l; Minn. Stat. Ann. § 13.386.

49 740 Ill. Comp. Stat. 14/1 – 14/99; Tex. Bus. & Com. Code Ann. § 503.001; Wash. Rev. Code §§ 19.375.010–19.375.900.

50 *See, e.g.*, N.Y. Gen. Bus. Law § 899-bb.

51 *See, e.g.*, Cal. Civ. Code §§ 1798.100–1798.199.

52 *See, e.g.*, City of Portland, Or., Ordinance No. 703 and 704 (2020).

53 *See, e.g.*, Cal. Health & Safety Code § 123115.

54 *See generally* U.S. Dep't of Health & Hum. Servs. Off. for C.R., Sharing Consumer Health Information? Look to HIPAA and the FTC Act, https://www.hhs.gov/sites/default/files/pdf-0219_sharing-health-info-hippa-ftcact%20508.pdf (last visited June 3, 2021).

55 *See* Cal. Civ. Code § 1798.145(c)(1)(a)&(b).

56 *See* Fed. Trade Comm'n, *Protecting Consumer Privacy and Security*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Mar. 10, 2020).

57 *See* Fed. Trade Comm'n, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 10, 2020).

58 *See* 15 U.S.C. § 45(a)(1).

59 *See id.* § 1681s.

60 *See id.* § 6805(a)(7).

61 *See* 47 U.S.C. § 227(b)(3); Mims v. Arrow Fin. Servs., LLC, 132 S.Ct. 740, 752–53 (2012).

62 *See* 16 C.F.R. pt. 318.

63 *See id.*

64 *See id.* § 318.1(a).

65 *See* 45 C.F.R. §§ 164.400–414.

66 Complaint at 1-3, Flo Health, Inc., F.T.C. File No. 1923133 (2021).

67 *Id.*

68 Agreement Containing Consent Order at 3-4, Flo Health, Inc., F.T.C. File No. 1923133 (2021).

69 *Id.* at 4.

70 *Id.*

71 Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394.

72 *See* 47 C.F.R. § 64.1200–1203.

73 *See generally* 47 U.S.C. § 227; 47 C.F.R. pts. 64 and 68.

74 *See generally* 47 U.S.C. § 227; 47 C.F.R. pts. 64 and 68.

75 *See* 47 C.F.R. § 64.1200(a)(9)(iv).

76 *See* 47 U.S.C. § 227(e)(5)).

77 *See id.* § 227(g)(1)&(2).

78 *See* 15 U.S.C. § 6505(a).

79 Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699.

80 *See* 16 C.F.R. pt. 316.

81 15 U.S.C. § 7702(2) (definition of "Commercial Electronic Mail Message").

82 *See* 16 C.F.R. § 1.98.

83 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100–1798.199.100.

84 *See* Cal. Code. Regs., tit. 11, ch. 20.

85 *See* Cal. Civ. Code § 1798.100.

86 *See id.* § 1798.100(d).

87 *See id.* § 1798.105.

88 *See id.* § 1798.130(a)(3)(B)(iii).

89 *See id.* § 1798.120.

90 *See id.* § 1798.125.

91 *See id.* § 1798.145(c)(A).

92 *See id.* § 1798.145(c)(B).

93 *See id.* § 1798.155(a).

94 *See id.* § 1798.150.

95 *See id.* § 1798.150(a)(1)(A).

96 *See* 45 C.F.R. § 46.102 (defining "Human Subject" as including a living individual about whom an investigator "[o]btains, uses, studies, analyzes, or generates identifiable private information").

97 *Id.* § 46.101.

98 21 C.F.R. § 50.3(c).

99 Cal. Health & Safety Code §§ 24000–26250.

100 Md. Code Ann., Health – Gen., §§ 13-2002–13-2004.

101 N.Y. Pub. Health Law §§ 2440–2446.

102 *See, e.g.*, Md. Code Ann., Health – Gen., § 13-2002(a).

103 *See, e.g.*, N.Y. Pub. Health Law § 2445(1).

104 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

105 *See id.* art. 4(1).

106 *See id.* recital 26.

107 *See id.* art. 4(1).

108 *See id.*

109 *See id.* art. 83(4).

110 *See id.*

111 *See id.* art. 83(5).

112 *See id.*

113 Lei Geral de Proteção de Dados Pessoais, Lei No. 13.709 de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 8.15.2008 (Braz.).

114 Privacy Protection Law, 5741-1981, LSI 35 136 (5741-1980/81).

115 Georg Disterer, *ISO/IEC 27000, 27001 and 27002 for Information Security Management*, 4 J. Info. Sec. 2, 92-100 (2013).

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.*

120 45 C.F.R. § 164.502.

121 *Id.* § 164.504(e).

122 *See* U.S. Dep't of Health & Hum. Servs., *Sign Up for the OCR Privacy & Security Listserv*, https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html (last visited June 24, 2021).

123 *See* Healthcare Info Sec., www.healthcareinfosecurity.com (last visited June 24, 2021).

124 This is an influential EU body comprised of representatives from each EU member state. Their website can be found at https://edpb.europa.eu/edpb_en.

125 *See* Eur. Data Prot. Supervisor, https://edps.europa.eu/ (last visited June 24, 2021).

126 *See generally* Atul Gawande, The Checklist Manifesto (2010).

127 The latest draft text can be found here: https://data.consilium.europa.eu/doc/document/ST-5979-2020-INIT/en/pdf. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)* 5979/20, (Feb. 21, 2020).

128 In accordance with GDPR *supra* note 104, at art. 28.

129 Venky Anant et al., *The Consumer-data Opportunity and the Privacy Imperative*, Mckinsey & Co. (Apr. 27, 2020), https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.

130 *See, e.g.*, 45 C.F.R. § 164.524; GDPR *supra* note 104, at art. 15.

131 *See, e.g.*, GDPR *supra* note 104, at art. 20.

132 *See, e.g.*, 45 C.F.R. § 164.526.

133 *See, e.g.*, GDPR *supra* note 104, at art. 16.

134 *See, e.g.*, 45 C.F.R. § 164.528; Cal. Civ. Code § 1798.110.

135 *See, e.g.*, 45 C.F.R. § 164.522(a).

136 *See, e.g.*, GDPR *supra* note 104, at art. 18.

137 *See, e.g.*, 45 C.F.R. § 164.522(b).

138 *See, e.g.*, GDPR *supra* note 104, at art. 21.

139 *See, e.g.*, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L. 201); Cal. Civ. Code § 1798.135.

140 47 C.F.R. § 64.1200(a).

141 *See, e.g.*, GDPR *supra* note 104, at art. 17; Cal. Civ. Code § 1798.105.

142 *See, e.g.*, GDPR *supra* note 104, at art. 7(3).

143 *See, e.g., id.* art. 77.

144 A "designated record set" is a group of records maintained by or for a covered entity that comprises the: (i) medical records and billing records about individuals maintained by or for a covered health care provider; (ii) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) other records that are used, in whole or in part, by or for the Covered Entity to make decisions about individuals. This last category includes records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access. *See* 45 C.F.R. § 164.501.

145 *See* 45 C.F.R. § 164.524; 45 C.F.R. § 164.522; 45 C.F.R. § 164.526; 45 C.F.R. § 164.528.

146 *See* U.S. Dep't of Health & Hum. Servs., *OCR Settles Eighteenth Investigation in HIPAA Right of Access Initiative*, (Mar. 26, 2021) https://www.hhs.gov/about/news/2021/03/26/ocr-settles-eighteenth-investigation-hipaa-right-access-initiative.html.

147 45 C.F.R. § 164.524.

148 *See, e.g.*, 45 C.F.R. § 164.308(a)(5).

149 These requirements can be found in Article 29 Working Party WP 248 rev.01 established by Article 29 of the Directive 95/46/EC and in guidance issued by local regulators, including the ICO.

150 *Data Governance – Glossary*, Nat'l Inst. Standards & Tech., https://csrc.nist.gov/glossary/term/data_governance.

151 Note that these rules do not squarely use the definition of PHI, but rather create and use the term EHI, which is defined to mean electronic protected health information as defined in 45 CFR § 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR § 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR § 160.103, but EHI shall not include: (1) Psychotherapy notes as defined in 45 CFR § 164.501; or (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. *See* 45 CFR § 171.102.

152 45 C.F.R. § 171.103(a).

153 *Id.* § 171.200.

154 *See* U.S. Dep't of Health & Hum. Servs., *Sign Up for the OCR Privacy & Security Listserv*, https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html (last visited June 24, 2021).

155 *See* IAPP, *Connect*, https://iapp.org/connect/ (last visited June 24, 2021).

156 *See* Healthcare Info Sec., www.healthcareinfosecurity.com (last visited June 24, 2021).

157 This is an influential EU body comprised of representatives from each EU member state. Their website can be found at https://edpb.europa.eu/edpb_en.

158 *See* Euro. Data Prot. Supervisor, https://edps.europa.eu/ (last visited June 24, 2021).

159 *See* Krebs on Security, https://krebsonsecurity.com/ (last visited June 24, 2021).