Microsoft

GDPR Compliance

GDPR Implementation and HIPAA Compliance: An Analysis of the GDPR and HIPAA for U.S. Health & Life Sciences Organizations

Hemant Pathak, Assistant General Counsel, Lead Attorney for Microsoft U.S. Sales & Marketing

Steve Mutkoski, Director of Government Affairs & Microsoft Worldwide Health

Nathan Leong, Lead Attorney, Microsoft U.S. Health & Life Sciences

Jackie Haydock, Attorney, Microsoft U.S. Health & Life Sciences

Melanie Scott-Bennett, Attorney, Microsoft U.S. Health & Life Sciences

Lisa J. Acevedo, Shareholder, Polsinelli, P.C.

Kathleen D. Kenney, Associate, Polsinelli, P.C.

Lindsay R. Dailey, Associate, Polsinelli, P.C.

GDPR implementation is a marathon, not a sprint, and requires the dedication of significant time and resources to ensure preparedness. U.S. Health & Life Sciences organizations that are already governed by HIPAA have a solid foundation of privacy and legal compliance experience when it comes to GDPR implementation. While these U.S. Health & Life Sciences organizations will greatly benefit from a strong compliance mindset, they must still take into account the different requirements posed by the GDPR. As the May 25, 2018 enforcement date quickly approaches, Microsoft and Polsinelli, P.C., have co-authored a white paper and blog series comparing and contrasting key GDPR requirements with their counterparts under HIPAA. These resources are intended to provide practical tips for U.S. Health & Life Sciences organizations for GDPR implementation, as well as GDPR applicability and compliance.

Microsoft

POLSINELLI

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

Introduction

The Health & Life Sciences Industry is highly regulated and complex. Successful organizations (including health care providers, payors, and industry service providers) that operate in this industry are well versed in navigating compliance and regulatory requirements. Health & Life Sciences organizations in the U.S. are experienced and proficient in complying with laws governing their products and services, including U.S. federal laws and regulations, such as the Health Insurance Portability and Accountability Act of 1996[1] (HIPAA) and its implementing regulations.

Traditionally, the regulation of health care in the United States has been viewed as location-specific, with U.S. Health & Life Sciences organizations governed under applicable U.S. federal laws, along with those of the states in which they have offices or sites of service. With the advent of the digital age and proliferation of online data collection, those geographic boundaries have blurred. Nowhere has the impact of this blurring of geographic boundaries been more evident than in the context of information privacy and security, and specifically with enactment of the European Union's General Data Protection Regulation[2] (GDPR). The GDPR imposes new rules on companies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR can apply no matter where you are located and may require compliance by U.S. Health & Life Sciences organizations who otherwise have not been subject to similar global laws.

The GDPR and HIPAA share many common themes and principles. Both are comprehensive regulatory schemes, each with the same overarching goal to protect individual privacy. Both regulate how covered information can be used, disclosed, maintained and transmitted, as well as how it must be secured. Both also provide individuals with certain rights to their data. Both regulate downstream vendors and both have breach reporting requirements.

However, despite the similarities and overlap between the GDPR and HIPAA, there are **critical differences** that U.S. Health & Life Science organizations should consider and address, including the scope of regulated individuals/entities, types of data regulated, and permitted uses and disclosures of regulated data.

The focus of this white paper is to address the applicability of the GDPR to U.S. Health & Life Sciences organizations and provide tips for GDPR applicability, implementation and compliance in the context of the general existing HIPAA compliance programs U.S. Health & Life Sciences organizations should already maintain. U.S. Health & Life Sciences organizations impacted by the GDPR, particularly those who act as HIPAA Covered Entities or Business Associates, will have a solid foundation of privacy and legal compliance when it comes to GDPR implementation. These U.S. Health & Life Sciences organizations will greatly benefit from their strong compliance mindsets when addressing the requirements unique to the GDPR.

At Microsoft, we value privacy as a fundamental right and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. Given the broad applicability and scope of the GDPR requirements, the journey to compliance may seem challenging, especially for U.S. based Health & Life Sciences organizations, and this white paper will hopefully provide background and context on the GDPR by comparing and contrasting a U.S. regulation very familiar to the industry - HIPAA. We will refer to terms (usually capitalized) throughout this white paper, which are defined in **Attachment 1**.

What is GDPR?

The GDPR is a regulation intended to harmonize data protection requirements across the European Union. It provides individuals with more control over their Personal Data, ensures transparency about the use of such data, and requires security and administrative controls to protect Personal Data. GDPR takes effect on May 25, 2018. It replaces the Data Protection Directive (Directive 95/46/EC), which has been in force since 1995. The GDPR actually became law in the EU in April 2016, but given the significant changes some organizations needed to make to align with the regulation, a two-year transition period was included. Want to read more about the GDPR generally? View additional Microsoft resources here.

Does the GDPR apply to U.S. Health & Life Sciences Organizations?

Yes, the GDPR can apply to U.S. Health & Life Sciences organizations under three different scenarios, none of which necessarily requires them to maintain sites of service or offices in the EU. This extra-territorial reach of the GDPR differentiates it from the previous European privacy regime. Specifically, the GDPR can apply to U.S. Health & Life Sciences organizations that are considered to have an "establishment" in the EU, which does not necessarily mean having an EU corporate entity. It can also apply to U.S. Health & Life Sciences organizations that do not have any physical presence in the EU, if they offer goods or services to EU residents. Finally, the GDPR can apply to U.S. Health & Life Science organizations that monitor the behavior of EU data subjects within the EU.[3]

Can the GDPR still apply to a "Non-EU Established" U.S. Health & Life Sciences Organization?

The definitions and terms that apply to determine the applicability of the GDPR are broad. For some U.S. Health & Life Sciences organizations, the determination as to whether GDPR will apply is a fairly straightforward analysis. However, for others, the analysis will be complex and may not be entirely clear. Consider these frequently asked questions when analyzing whether the GDPR applies to your organization:

> **Question 1**: We have a website that EU residents can access. Does the fact that EU residents may access our site mean that any Personal Data we collect on that site from EU residents is governed by the GDPR?
>
> **Answer**: No, the GDPR will likely only be triggered if the site would be considered to be directed to EU data subjects. Examples of language on a site that might suggest that the site is directed to EU data subjects could include the use of EU country-specific language or EU currency to facilitate the ability of EU data subjects to place orders via the site. This is a case-by-case analysis. However, if you are collecting data from EU residents to monitor their online behavior, then the GDPR may apply.
>
> **Question 2**: We don't have corporate offices in the EU, but we do have independent contractors who provide services to some EU businesses with which we have relationships. Does this mean we are governed by the GDPR?
>
> **Answer**: It depends. It is not clear whether offering goods or services to EU businesses rather than to EU data subjects will trigger the GDPR, but having independent contractors in the EU acting on behalf of the

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

organization could trigger the GDPR. This is a complex analysis and we recommend seeking the advice of legal counsel.

Question 3: Our website collects the IP addresses of all visitors, including those in the EU. Does that mean we are governed by the GDPR?

Answer: An IP address is considered to be Personal Data under the GDPR.[4] If you are using the data to track EU data subjects online or create profiles about them or are otherwise Processing IP addresses of EU data subjects, you may be subject to the GDPR.

What types of data are regulated by the GDPR and do they overlap with the scope of data regulated by HIPAA?

Key Takeaways

U.S. Health & Life Sciences organizations that are governed by HIPAA may have a head start with their GDPR implementation because they have experience in implementing broad privacy and security compliance programs, and this experience will provide the foundation for their GDPR compliance program. However, given the broader range of implicated Personal Data under the GDPR, they should map all of their data flows that trigger the GDPR and create an inventory of such data, including recording the Processing activities associated with the Personal Data, and implement GDPR-relevant controls.

HIPAA governs the use and disclosure of Protected Health Information by Covered Entities and their Business Associates. HIPAA applies to Covered Entities, defined as health care providers who engage in certain electronic standard transactions, health plans and health care clearinghouses, as well as the Business Associates of these Covered Entities, which essentially are the vendors and services providers who must use, disclose, have access to, or maintain Protected Health Information (PHI) in order to perform their services. HIPAA regulates the use, disclosure, and protection of Protected Health Information by these entities. HIPAA does not apply to all the personal information that a Covered Entity or Business Associate may hold; it only applies to information that fits within the definition of Protected Health Information.

On the contrary, the GDPR broadly regulates the "Processing" of "Personal Data" by any entity that falls within the scope of the GDPR. This means that the GDPR regulates the collection, use, disclosure, recording, storage, maintenance structuring, adaptation, alteration, retrieval, consultation, and transmission of ALL PERSONAL DATA, which is a broader scope of data than health data or financial data or other specific categories of data that are regulated under U.S. privacy laws, including Protected Health Information (as defined by HIPAA). Unlike HIPAA, the GDPR applies broadly to any entity engaged in Processing of Personal Data.

In summary, the scope of data covered by GDPR is **significantly broader** than HIPAA.

Does the GDPR restrict uses and disclosures of Personal Data in the same manner as HIPAA?

Both the GDPR and HIPAA are similar in that each regulatory scheme is essentially structured to prohibit uses and disclosures of covered information, unless there is a specific provision in the regulation that permits it. Specifically, HIPAA prohibits uses and disclosures of PHI unless there is a valid exception under HIPAA for doing so. The GDPR similarly restricts the Processing of Personal Data. That being said, data Processing under the GDPR is **more restrictive** than what U.S. Health & Life Sciences organizations might be familiar with under HIPAA.

The GDPR characterizes its restrictions on uses and disclosures of Personal Data as requiring entities to have a lawful reason to permit Processing.[5] In other words, a U.S. Health & Life Sciences organization that is governed under the GDPR is only

permitted to process Personal Data as lawfully permitted under the GDPR. The lawfully permitted purposes under the GDPR are not as numerous as the exceptions under HIPAA. Nor is their potential applicability as specific to the underlying facts and circumstances as are the exceptions under HIPAA. For example, one lawfully permitted purpose for Processing Personal Data under the GDPR is if the Processing is in the "legitimate interests" of the company.[6] While there is some guidance as to what constitutes "legitimate interests," the GDPR does not generally list out the specific types of activities that fall within this category.

Does the GDPR regulate Health Data in the same manner as HIPAA?

The GDPR imposes more strict conditions on the Processing of "sensitive" categories of Personal Data, which include health, biometric and genetic data, but such categories also include other types of data unrelated to health, such as race, ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership.[7] The list of lawfully permitted purposes for Processing sensitive categories of Personal Data is different than that of non-sensitive Personal Data.

Unlike the GDPR, HIPAA, by and large, does not regulate different types of PHI in a different manner, meaning demographic information is restricted in the same manner as full clinical data (with the exception of special protections for Psychotherapy Notes and genetic information for underwriting purposes).

How do the lawfully permitted purposes for disclosure under the GDPR compare to the exceptions under HIPAA?

The GDPR only permits Processing of Personal Data if the underlying purpose for Processing is supported by a lawful reason, whereas HIPAA contains broad exceptions that permit disclosures for purposes of payment and health care operations, along with a host of other exceptions not directly contemplated in the GDPR. There is some overlap between the GDPR and HIPAA for a number of permitted Processing purposes, however, for the most part, there are significant differences between the various lawful reasons/exceptions permitting disclosure, such that a case-by-case analysis must be conducted to determine if a use or disclosures permissible under HIPAA is also permissible under the GDPR, and vice versa.

A more detailed analysis of the lawful reasons for Processing sensitive Personal Data and a comparison of potentially comparable exceptions under HIPAA is included in **Attachment 2**.

Key Takeaways

Given the material differences between the GDPR and HIPAA, organizations should conduct a case-by-case analysis to determine if a use or disclosure under HIPAA is also permissible under GDPR and vice versa. To operationalize the restrictions on Processing sensitive Personal Data, organizations should map their EU sensitive Personal Data and evaluate the potential lawful reasons on which they rely to justify the Processing. Note also that the GDPR permits EU Member States to impose further conditions and restrictions on the Processing of health, genetic and biometric data.[8] As a result, U.S. Health & Life Sciences organizations must take care to consult local laws governing these categories of sensitive Personal Data in the applicable EU jurisdiction.

How does the treatment of individual rights compare under the GDPR and HIPAA

Like HIPAA, the GDPR provides people whose data are processed, known as data subjects, with certain rights when it comes to their Personal Data and imposes a timeframe for responding to requests to exercise such rights. The GDPR imposes these requirements on "Controllers" which are the organizations that determine the

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

purposes and means for Processing Personal Data[9] and most closely mirror HIPAA Covered Entities. GDPR mandates that Controllers provide responses to certain data subject requests without unreasonable delay and within one month of receipt of a request (with an opportunity, if necessary, for an extension).[10]

A data subject has the right under the GDPR to request access to his/her Personal Data – similar to the right to access PHI under HIPAA. To the extent an access request is made electronically under the GDPR, the information must be provided in a commonly used electronic form unless requested in another format by the data subject.[11]

In addition, similar to an individual's right to request an amendment under HIPAA, the GDPR provides data subjects with a right to request rectification. Specifically, data subjects have the right under the GDPR to request that a Controller correct Personal Data stored about them or, to the extent Personal Data is incorrect or incomplete, request that the Controller complete the incorrect or incomplete record of such Personal Data or record a supplementary statement, where applicable.[12]

The following individual rights under the GDPR also bear similarities to HIPAA's individual rights: (i) the right to be informed about how Personal Data is being used[13] and (ii) the right to be provided with supplemental information about the data Processing under the GDPR's access right.[14]

Key Takeaways

To operationalize the rights afforded to data subjects under the GDPR, U.S. Health & Life Sciences organizations should review and build upon their privacy program policies and procedures governing implementation of individual rights under HIPAA. Additionally, given the additional rights afforded under the GDPR, U.S. Health & Life Sciences organizations should create new policies and procedures and train employees on these new rights.

Are there differences between breach reporting under the GDPR and HIPAA?

Like HIPAA, the GDPR requires Controllers to provide notification of a breach to a regulatory body within a specific timeframe.[15] The GDPR also requires Controllers to provide notification to data subjects in certain circumstances – much like HIPAA requires Covered Entities to notify affected individuals if an incident rises to the level of a reportable breach.[16] In a manner similar to HIPAA, a Controller's vendors, referred to as Processors, which are like Business Associates, must notify Controllers of their breaches.[17]

However, the thresholds for triggering breach reporting obligations under HIPAA and the GDPR differ. Under the GDPR, a Controller must notify the supervisory authority unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[18] Notification to data subjects must be provided when the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons.[19] HIPAA, on the other hand, provides that a Breach of Unsecured PHI is presumed to be reportable (to individuals and the Office for Civil Rights) unless the Covered Entity can demonstrate that there is a low probability that the PHI was compromised through application of a four factor risk assessment. Thus, HIPAA relies on a more objective analysis of the likelihood that the data was compromised, while the GDPR focuses more subjectively on the potential risk of harm to the data subject.

Notification timelines under the GDPR are more stringent than HIPAA, which requires notification without unreasonable delay and in no case later than sixty (60) days.[20] Under the GDPR, Controllers must notify supervisory authorities "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[21] Additionally, under the GDPR, if notification is not made within 72 hours, the Controller must provide a "reasoned justification" for the delay.[22] Notice to affected individuals should be made "without undue delay."[23]

Key Takeaways

U.S. Health & Life Sciences organizations that are governed by HIPAA and also subject to the GDPR breach reporting requirements should be well-positioned to adjust to the new (and even differing) obligations and operationalize the GDPR breach requirements. They should also evaluate cyber insurance policies to ensure Personal Data breaches as defined by the GDPR will be covered. Importantly, they should train their workforce on identifying and reporting a Personal Data breach under the GDPR given the much shorter (72-hour) timeframe for reporting.

How do the compliance program obligations under the GDPR compare to those required under HIPAA?

Vendor Management

Both the GDPR and HIPAA require organizations to manage and contractually bind their vendors (i.e., Business Associates and Processors) to certain standards and terms.[24] Although each regulation has different required language for such contracts, the concept of vendor management is seen in both regulations.

Record of Processing Activities

Unlike HIPAA, the GDPR requires Controllers to maintain an ongoing record of their specific Processing activities, including the type of Personal Data processed and the purposes for which it is processed. Similarly, Processors must maintain records about the Personal Data they process on behalf of Controllers. Keeping this record will require creating and maintaining an inventory of all Processing activities, which will require significant effort.

Privacy by Design & DPIAs

The Privacy by Design and Data Protection Impact Assessment (DPIA) concepts and processes are unique to the GDPR, however the underlying principles are similar to and also inherent in HIPAA.

Privacy by Design requires organizations to proactively consider and address data protection through implementation of appropriate technical and organizational measures at the outset of product or service development.[25] HIPAA addresses this concept indirectly through the Security Rule's requirements for implementation of technical, administrative, and physical safeguards to protect electronic PHI, and through the Privacy Rule's requirement that only the minimum amount of PHI necessary be used or disclosed to accomplish a given task.

The GDPR prescribes a specific process for organizations to undertake and proactively implement before certain types of Processing activities can begin. Specifically, the GDPR requires DPIAs be completed for any "high risk" Processing activities before such activities can begin.[26] At a minimum, a DPIA must address: (i) a description of the Processing operations and purpose of Processing; (ii) an assessment of the need for and proportionality of the Processing, and the risks to data subjects (viewed from the perspective of the data subject); and (iii) a list of the measures to mitigate those risks and ensure compliance with the GDPR.[27]

Key Takeaways

The GDPR's obligations overlap HIPAA compliance program requirements but include a level of specificity in some cases not found in HIPAA. To address the GDPR's requirements governing Processors, Covered Entities should build upon their current infrastructure to include Processors in their inventory of Business Associates (and Business Associates should build upon their infrastructure to include GDPR subprocessors in their inventory of Subcontractors). With regard to Privacy by Design and DPIAs, although HIPAA addresses the underlying principles of these requirements, the GDPR requirements are unique enough that U.S. Health & Life Sciences organizations will need to build new processes and documentation around these. Although there is no template DPIA form, developing and customizing one for your organization can assist with streamlining this process and creating consistency in your approach. Integrating Privacy by Design and the DPIA process into your organization's intake, new business development, and new Personal Data collection/Processing activities, along with training personnel, is key to help enable compliance.

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

Key Takeaways

U.S. Health & Life Sciences companies that already have implemented a robust HIPAA Security Rule compliance program and have systems and processes compliant with the HIPAA Security Rule will have a head start in building and implementing GDPR-specific programs, systems, and processes for security. One challenge will be that the GDPR applies more broadly than just to PHI, so U.S. Health & Life Sciences organizations will likely have to expand their security programs to other data not regulated by HIPAA but governed by the GDPR, e.g., Personal Data of EU employees maintained by the organization in its role as an employer.

How do security requirements under GDPR compare to the HIPAA Security Rule?

Both the GDPR and the HIPAA Security Rule require implementation of appropriate technical and administrative measures to protect the confidentiality, integrity and availability of covered data. They both also broadly require an assessment of the risks to data against the measures designed to protect data to determine if additional protections need to be addressed. However, the GDPR requirements related to security are very broad and do not address specific security requirements to the degree that the HIPAA Security Rule does. The fact that the HIPAA Security Rule comprises multiple separate standards and implementation specifications for each of the administrative, physical, and technical safeguards, all of which comprise multiple pages of regulations, while the security requirements in the GDPR are set forth in one Article, which is only comprised of four paragraphs, illustrates the difference in the level of detail. Compliance with the HIPAA Security Rule should provide a good foundation of expertise and knowledge for U.S. Health & Life Sciences organizations to apply to their GDPR security compliance journey.

How do non-compliance penalities compare under the GDPR and HIPAA?

HIPAA violations can be pursued in the U.S. by both State and Federal regulators, and failures to comply with HIPAA requirements can result in both civil and criminal penalties.[28] Civil monetary penalties are determined through a tiered penalty structure based on a regulator determination of the facts, circumstances and egregiousness of the violation, and the resulting harm.[29] For example, an unknowing innocuous violation may result in fines of $100 per violation with an annual maximum of $1.5 million dollars for identical violations.[30] However, willful breaches can result in $50,000 per violation, with an annual maximum of $1.5 million dollars per violation.[31] Penalties can be cumulative depending on the nature and number of individuals affected by the violation, and multi-million dollar settlements are not historically uncommon in the U.S.[32] HIPAA violations can also result in criminal penalties ranging from one year imprisonment for unknowing violations up to 10 years imprisonment for violations for personal gain or malicious reasons.[33]

Key Takeaways

Penalties under both HIPAA and GDPR compliance violations can be significant for U.S. Health & Life Sciences organizations. Drastic monetary penalties, and potential for criminal sanctions, could cause permanent damage to their business. Even in the event that the business could absorb such penalties related to non-compliance, incidental costs associated with legal fees, investigation, remediation and public relations would also have to be absorbed. Further, the long lasting reputational harm could result from the failure to protect Personal Data or PHI in compliance with HIPAA and the GDPR.

Penalties for violation of GDPR can also result in drastic consequences. The extent and severity of supervisory enforcement does not yet have an established baseline for analysis. However, the GDPR provides member state supervisory authorities with the latitude to levy administrative fines up to an amount of €10 million, or 2% of global annual revenue, whichever is greater, for GDPR violations related to design failures such as failing to implement appropriate technical safeguards and other failures related to certain requirements.[34] The fines double to €20 million or 4% of global revenue, whichever is greater, for scenarios involving the violation of core GDPR principles such as data subject rights and/or basic principles for Processing, including requirements related to consent, and impermissible cross-border transfers of Personal Data.[35] Member states also retain the discretion to enact

criminal penalties for those violations of the GDPR for which there is not an administrative penalty or for egregious GDPR violations.[36]

What is Microsoft's commitment to GDPR compliance?

Microsoft has a long and demonstrated history of partnering with industry customers to address compliance requirements as an embedded component of its products and services. Microsoft was the first major cloud vendor to offer a HIPAA Business Associate Agreement to help its U.S. Health & Life Sciences customers address their compliance requirements prior to migrating their regulated Protected Health Information into our cloud. That industry collaboration and compliance commitment is continuing not only with respect to our next generation of product and services releases, but also with regard to rapidly changing laws and regulations worldwide. We are committed to GDPR compliance across our cloud services when enforcement begins May 25, 2018, and, as we did with HIPAA, we will be steadfast in maintaining that compliance and providing contractual stipulations to not only assure our customers, but also help them address their own GDPR compliance requirements. Learn more about how our products help you comply with the GDPR, and let us help you get started. You can also find resources like webinars, videos, white papers, and FAQs about the regulation.

* * * * * *

Disclaimer

This white paper is a commentary on the GDPR and HIPAA, as Microsoft interprets them, as of the date of publication. The application of the GDPR and of HIPAA are highly fact-specific, and not all aspects and interpretations of the GDPR are well-settled. As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how the GDPR and HIPAA might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss the GDPR and HIPAA, how they apply specifically to your organization, and how best to ensure compliance. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS WHITE PAPER. This white paper is provided "as-is." Information and views expressed in this white paper, including URL and other Internet website references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this white paper for your internal, reference purposes only.

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. The choice of a lawyer is an important decision and should not be based solely upon advertisements.

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

ATTACHMENT 1

Glossary of Key Words

GDPR

Controller - The entity that determines the purposes, conditions and means of the Processing of Personal Data. Article 4(7).

Data Erasure - Also known as the right to be forgotten, it entitles the data subject to have the Controller erase his/her Personal Data, cease further dissemination of the data, and potentially have third parties cease Processing of the data. See Article 17.

Data Protection Impact Assessment or DPIA - A tool used to identify and reduce the privacy risks to Personal Data by analyzing the Personal Data to be processed and the protections in place. See Article 35.

GDPR - General Data Protection Regulation. Regulation (EU) 2016/678 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.

Personal Data - Any information related to a natural person that can be used to directly or indirectly identify the person. Article 4(1).

Privacy by Design - A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than a subsequent addition. Article 25.

Processor - The entity that processes data on behalf of the Controller. Article 4(8).

Processing - Any operation performed on Personal Data, whether or not by automated means, including collection, use, recording, etc. Article 4(2).

HIPAA

Breach - The unauthorized acquisition, access, use, or disclosure of unsecured PHI, which compromises the security or privacy of such information. 45 C.F.R. § 164.402.

Business Associate - An entity that performs certain services for or on behalf of a Covered Entity and creates, receives, maintains or transmits PHI to do so. 45 C.F.R. § 160.103.

Covered Entity - A health care provider that engages in HIPAA electronic standard transactions, a health plan or a health care clearinghouse. 45 C.F.R. § 160.103.

HIPAA - The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, and the regulations that implement HIPAA.

HIPAA Privacy Rule - The Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E.

HIPAA Security Rule - The Security Standards for the Protection of Electronic PHI at 45 C.F.R. Parts 160 and 164, Subparts A and C.

Individually Identifiable Health Information - Information created or received by a Covered Entity that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care, and that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, such as names, dates, phone/fax numbers, e-mail addresses, home addresses, social security numbers and demographic data. 45 C.F.R. § 160.103.

Protected Health Information or PHI - Individually Identifiable Health Information (defined above) maintained or transmitted in any form or medium that is created or received by or from a Covered Entity. 45 C.F.R. § 160.103.

ATTACHMENT 2

Permissible Reason For Disclosure Comparison Chart

Permissible Reason for Processing Sensitive Data	GDPR	HIPAA	Comparison of GDPR vs. HIPAA
Explicit Consent	Processing of sensitive Personal Data is permissible with explicit consent of the data subject unless reliance on consent is prohibited by EU or Member State Law. In addition, to be valid, a consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes. GDPR emphasizes a new condition, which is that a consent will not be valid if there is a clear imbalance of power between the data subject and Controller. The GDPR requires consents to be distinguishable, meaning consent language must be sufficiently separate from other written terms, agreements or matters in a document. GDPR consent must be revocable (in a manner as easy as consent was given) and it must be granular, meaning there must be sufficient detail regarding the specific Processing to enable the data subjects to give informed consent.	HIPAA permits disclosures of PHI pursuant to a valid authorization. To be valid an authorization must meet HIPAA's content requirements, some of which are similar to the GDPR explicit consent requirements.	A consent that would be effective under the GDPR might not constitute a valid HIPAA authorization because the GDPR requirements are not nearly as specific as the required elements that must be present for an authorization to be valid under HIPAA. Organizations relying on explicit consents under either law should confirm that such consent has the requisite elements.
Vital Interests of Data Subject	The Processing is necessary to protect vital interests of the data subject (or another person) where the data subject is physically or legally incapable of giving consent.	HIPAA permits disclosures to friends, family and others involved in a patient's care or payment for that care under certain circumstances, including where the patient is either not present or is incapacitated. In the event of incapacity, HIPAA also permits certain individuals to act as the patient's personal representative and such individuals can make decisions on behalf of such individuals including providing authorization to disclosures. HIPAA also has an exception that permits disclosures, as necessary, to prevent or lessen a serious and imminent threat to the health or safety of the patient or public under certain circumstances.	HIPAA might permit disclosures that would fit within this permissible purpose for Processing under the GDPR, but the HIPAA exceptions are more fact-specific so a case-by-case analysis must be conducted.

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

Permissible Reason for Processing Sensitive Data	GDPR	HIPAA	Comparison of GDPR vs. HIPAA
Processing by Not-For-Profit Organizations	The Processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes.	There is no comparable exception under HIPAA. The closest exception would be the exception that permits certain limited uses and disclosures of PHI for purposes of fundraising.	Additional information regarding the ultimate purposes would have to be obtained to determine if HIPAA would permit a use or disclosure under this lawfully permissible reason under GDPR.
Data Made Public	The Processing relates to Personal Data which have been manifestly made public by the data subject.	HIPAA takes the opposite approach and prohibits disclosure of information that meets the definition of PHI regardless whether that information has also been made public.	Not permitted under HIPAA.
Defense of Legal Claims or Judicial Proceedings	The Processing is necessary for the establishment, exercise or defense of legal claims, or for courts acting in their judicial capacity.	Defending against legal claims would be considered a permissible health care operations activity under HIPAA, and HIPAA also has an exception that permits disclosures of PHI in the course of judicial proceedings.	HIPAA contains additional and more detailed criteria for some disclosures that fit within the category of disclosures in the course of legal proceedings.
Substantial Public Interest	The Processing is necessary for reasons of substantial public interest, and occurs on the basis of Union or Member State law that is, among other things, proportionate to the aim pursued and protects the rights of data subjects.	There are a number of exceptions that permit disclosures as required or authorized by law, including disclosures related to public health activities, to report certain abuse, neglect or domestic violence, for oversight of the health care system and government benefits programs, among others. Each such exception contains criteria that must be met for the exception to apply.	Additional information regarding the ultimate purposes would have to be obtained to determine if HIPAA would permit a use or disclosure.

Permissible Reason for Processing Sensitive Data	GDPR	HIPAA	Comparison of GDPR vs. HIPAA
Medical Treatment	The Processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services on the basis of Union or Member State law or a contract with a health care professional.	Broadly permits disclosures for treatment purposes, including provision, coordination or management of health care and related services among health care providers or with a third party, care coordination and referrals from one provider to another.	The HIPAA exception for treatment purposes would not necessarily extend to the "management of health or social care systems or services" as permitted by the GDPR. Note that care must be taken when providing health care services to employees for employment purposes. Although the GDPR permits disclosures related to assessing the working capacity of employees, HIPAA generally requires authorization to disclose PHI to employers, with limited exceptions to permit an employer to comply with its OSHA obligations related to workplace safety and medical surveillance, and for workers' compensation compliance.
Public Health	The Processing is necessary for reasons of public interest in the area of public health (e.g., ensuring the quality and safety of medicinal products, protecting against cross-border threats to health).	As noted above, HIPAA also contains a broad exception that permits disclosures for public health purposes, including to public health authorities for purposes of controlling disease, and to manufacturers of drugs and devices regulated by the FDA for purposes of quality, safety or effectiveness of such drugs or devices.	Disclosures permitted under GDPR will likely be permitted under HIPAA.
Research	The Processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.	Permits uses and disclosures of PHI for research, defined broadly as a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge, subject to strict restrictions.	HIPAA contains numerous and specific criteria that must be followed to rely on the research exception.
Employment, Social Security/ Protection Law or Collective Agreement	The Processing is necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement.	As mentioned above, HIPAA generally disfavors disclosures of PHI to employers, with limited exceptions for workplace surveillance and health under OSHA and for purposes of workers' compensation.	Additional information regarding the ultimate purposes would have to be obtained to determine if HIPAA would permit a use or disclosure.

© 2018 Microsoft Corporation, Polsinelli PC. All rights reserved.

NOTES

[1] 45 C.F.R. Parts 160 and 164.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Repealing 95/46/EC.

[3] Article 3(2)(b).

[4] Article 4(1).

[5] Article 6.

[6] Article 6(1)(f).

[7] Article 9.

[8] Recital 53.

[9] Article 4(7).

[10] Recital 59.

[11] Article 15(3).

[12] Article 16.

[13] Articles 12-14.

[14] Article 15(1)(c).

[15] Article 33.

[16] Article 34.

[17] Article 33(2).

[18] Article 33(1).

[19] Article 34(1).

[20] 45 C.F.R. § 164.404(b)

[21] Article 33(1).

[22] Id.

[23] Article 34(1).

[24] Article 28.

[25] Article 25.

[26] Article 35.

[27] Article 32.

[28] 45 C.F.R. § 160.400; 42 U.S.C. § 1320d–6.

[29] 45 C.F.R. § 160.402(b).

[30] 45 C.F.R. § 160.404(b)(2)(i).

[31] 45 C.F.R. § 160.404(b)(2)(iii).

[32] 45 C.F.R. § 160.406.

[33] 42 U.S.C. § 1320d–6(b).

[34] Article 83(4).

[35] Article 83(5).

[36] Article 84; Recital 152.