Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on

Advancing Privacy Enhancing Technologies

IQVIA Inc

July 8, 2022

Response for Request for Information (RFI) on Advancing Privacy-Enhancing Technologies

Submitted By: Kim Gray, Chief Privacy Officer, IQVIA Inc. (industry)

This response to the Request for Information on Advancing Privacy-Enhancing Technologies ("PETs") is submitted on behalf of IQVIA Inc. IQVIA™ (NYSE:IQV) is a leading global provider of advanced analytics, technology solutions and clinical research services to the life sciences industry. IQVIA is a global leader in protecting individual patient privacy. The company uses a wide variety of privacy-enhancing technologies and safeguards to protect individual privacy while generating and analyzing information on a scale that helps healthcare stakeholders identify disease patterns and correlate with the precise treatment path and therapy needed for better outcomes. IQVIA's insights and execution capabilities help biotech, medical device and pharmaceutical companies, medical researchers, government agencies, payers and other healthcare stakeholders tap into a deeper understanding of diseases, human behaviors and scientific advances, in an effort to advance their path toward cures. I am the Global Chief Privacy Officer for IQVIA.

The Office of Science and Technology Policy ("OSTP") is seeking information concerning privacy-enhancing technologies. The focus of my comments is on one kind of privacy-enhancing technology – the use of de-identification or anonymization techniques as a means of disconnecting information about individuals from the identity of those individuals, so that this information, in the health care sector and others, can be used for a broad variety of publicly beneficial purposes without sacrificing privacy protections. This technique can be used across industries and can serve to benefit the public overall through providing a means of broader access to data for research and analytical purposes while still protecting individual privacy. We encourage OSTP to endorse this approach and to provide additional means for companies, in the health care industry and more broadly, to utilize experts to facilitate the development of appropriately de-identified information.

In particular, we want to focus OSTP's attention on the de-identification standard of the Privacy Rule under the Health Insurance Portability and Accountability Act ("HIPAA"). This standard – one of the earliest legal standards in the United States related to this kind of technology – remains the gold standard for de-identification in the US legal system and beyond. We encourage the continued use of this standard in the health care industry generally and believe that its approach can serve as a model for other areas of our economic system. Under the HIPAA rules, the de-identification formula permits, for example, the linkage across data sets of patient level data in a way that permits longitudinal evaluation of the data (a patient's journey through the health care process over time) without any identification of the patient. It is important when conducting medical research or public health activities to know that the health data applies to the same patient, but is not important for much of this analytical activity to know who the patient is. Individual privacy is protected while health data research benefits everyone.

Background for the HIPAA De-Identification Standard

Following the passage of the Health Insurance Portability and Accountability Act of 1996, Public Law 104 – 19, the Department of Health and Human Services developed the Standards for Privacy of Individually Identifiable Health Information ("the HIPAA Privacy Rule").

Under the HIPAA Privacy Rule, HIPAA covered entities must provide privacy and security protection for "protected health information" ("PHI") – individually identifiable health information about patients and insureds. The substantive provisions of the HIPAA Privacy Rule were designed to provide appropriate privacy protection while still permitting the health care system to work effectively and efficiently, for the benefit of both patients and the health care industry (and society at large). For example, provisions of the HIPAA Privacy Rule were designed to make the "common" uses and disclosures of this protected health information seamless, focusing on uses and disclosures for treatment, payment and health care operations. Uses and disclosures beyond these common purposes require explicit patient permission. The goal of this approach was to facilitate the efficient operation of the health care system while also protecting individual privacy.

A similar approach was taken in connection with the de-identification of this PHI, as set forth in 45 C.F.R. § 164.514(a-b). In drafting the regulations, the United States Department of Health and Human Services ("HHS") recognized that the de-identification standard it developed could be even more patient protective, meaning almost no or no risk of re-identification of individuals rather than a low risk. However, when drafting these provisions and responding to public comments, HHS was explicit in acknowledging that this "no risk" additional protection offered only marginally more privacy protection and would come at the expense of a broad range of socially desirable uses and disclosures of this information. That led to the development of the HIPAA Privacy Rule de-identification standards, as a means of providing BOTH appropriate privacy protection and the socially desirable ability to use and disclose this "de-identified" information. Where this standard was met, "[r]egardless of the method by which de-identification is achieved, the [HIPAA] Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information." Consistent with the goals of this RFI, we encourage a broader incorporation of this concept by OSTP, in the health care industry generally (both in and out of the scope of HIPAA) as well as in a broader range of other industries.

The de-identification standard is a core element of the HIPAA Privacy Rule. In its primary guidance concerning this standard, the HHS Office for Civil Rights stated that "[t]he increasing adoption of health information technologies in the United States accelerates their potential to facilitate beneficial studies that combine large, complex data sets from multiple sources. The process of de-identification, by which identifiers are removed from the health information, mitigates privacy risks to individuals and thereby supports the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research, and other endeavors."[1]

The HIPAA Privacy Rule created two standards for de-identification – the "expert determination" method and the "safe harbor" method.

As set forth in this guidance, the HIPAA Privacy Rule "was designed to protect individually identifiable health information through permitting only certain uses and disclosures of PHI

[1] Department of Health and Human Service, Office for Civil Rights, "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule," https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf at 5 (November 2012).

provided by the [HIPAA Privacy] Rule, or as authorized by the individual subject of the information." However, "in recognition of the potential utility of health information even when it is not individually identifiable, § 164.502(d) of the [HIPAA] Privacy Rule permits a covered entity or its business associate to create information that is not individually identifiable by following the de-identification standard and implementation specifications in § 164.514(a)-(b)." By utilizing these provisions, a covered entity is allowed "to use and disclose information that neither identifies nor provides a reasonable basis to identify an individual."

Under this HIPAA de-identification standard, "health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual." As HHS has noted, "[b]oth methods, even when properly applied, yield de-identified data that retains some risk of identification. Although the risk is very small, it is not zero, and there is a possibility that de-identified data could be linked back to the identity of the patient to which it corresponds."

The first is the "expert determination" method. Under this approach, a covered entity may determine that health information is not individually identifiable health information only if:

A person, with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination.

The second is the "safe harbor" method. This method involves removal of a specific set of defined identifiers. "[I]dentifiers of the individual or of relatives, employers, or household members of the individual, are removed . . . as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual."

HHS has consistently acknowledged the key purposes of this rule. In early commentary for the HIPAA Privacy Rule, in discussing public comments (See 67 Federal Register 53232 (August 14, 2002), HHS noted:

> The Department is cognizant of the increasing capabilities and sophistication of electronic data matching used to link data elements from various sources and from which, therefore, individuals may be identified. Given this increasing risk to individuals' privacy, the Department included in the [HIPAA] Privacy Rule the above stringent standards for determining when information may flow unprotected. The Department also wanted the standards to be flexible enough so the [HIPAA] Privacy Rule would not be a disincentive for covered entities to use or disclose de-identified information wherever possible. The [HIPAA] Privacy Rule, therefore, strives to balance the need to protect individuals' identities with the need to allow deidentified databases to be useful.

Similarly, in the initial publication of the HIPAA Privacy Rule (see generally 65 Federal Register 82708 (December 28, 2000), HHS noted that:

> We also disagree with the comments that advocated using a standard which required removing only the direct identifiers. Although such an approach may be more convenient for covered entities, we judged that the resulting information would often remain identifiable, and its dissemination could result in significant violations of privacy. While we encourage covered entities to remove direct identifiers whenever possible as a method of enhancing privacy, we do not believe that the resulting information is sufficiently blinded as to permit its general dissemination without the protections provided by this rule.
>
> We agree with the comments that said that records of information about individuals cannot be truly deidentified, if that means that the probability of attribution to an individual must be absolutely zero. However, the statutory standard does not allow us to take such a position, but envisions a reasonable balance between risk of identification and usefulness of the information.
>
> We disagree with those comments that advocated releasing only truly anonymous information (which has been changed sufficiently so that it no longer represents actual information about real individuals) and those that supported using only sophisticated statistical analysis before allowing uncontrolled disclosures. Although these approaches would provide a marginally higher level of privacy protection, they would preclude many of the laudable and valuable uses discussed in the NPRM (in § 164.506(d)) and would impose too great a burden on less sophisticated covered entities to be justified by the small decrease in an already small risk of identification.

In the almost two decades since these provisions became final, the HIPAA de-identification method has become both a core element of the HIPAA rules and has provided both appropriate privacy protections and the ability for those in the health care industry and otherwise to benefit from a wide range of uses for de-identified data, including public health purposes, medical research and a wide range of additional commercial purposes. These benefits have been able to be achieved without any identifiable risks to the privacy of this personal information. The information is protected, privacy is maintained, and the public (and individuals) can benefit from these uses. We encourage OSTP to both reconfirm the validity of this approach as an important privacy-enhancing technology and to evaluate how best to apply this standard in the context of activities outside of the health care system, where the same benefits of privacy protection and beneficial data uses can be achieved.

Specific Questions from the RFI

Beyond this general discussion of the benefits of the HIPAA de-identification standard and how this standard can be used as a privacy enhancing technology in the health care system and otherwise, I wanted to discuss some additional points related to specific questions in the RFI.

- Specific research opportunities to advance PETs; Existing barriers to PET adoption (Questions 1 and 9)

The government can assist with the development of privacy-enhancing technologies by providing additional education and training related to potential experts for this de-identification approach. The HIPAA de-identification standard is useful and important; at the same time, because of its complexity to ensure that data is both useful and privacy protective, the expertise necessary to provide an "expert determination" is limited. The government can assist by providing additional means of developing appropriate experts. This can include government education and training in this area, as well as identifying more specific means for organizations to identify and utilize experts for these determinations. The limited number of experts in this field and the associated costs for an expert determination may be barriers to additional adoption of the HIPAA de-identification approach, even within the health care industry.

- Specific technical aspects or limitations of PETs (Question 2)

The government may be able to assist in this area by developing standard or automating means of implementing these requirements under the HIPAA rules. These standards would serve to supplement any additional education and training for potential experts, as well as help assist with the current economic burdens involved in paying for these expert determinations.

- Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs (Question 3)

The formal elements of the HIPAA de-identification standard are used, at this point, primarily within the health care industry, focused primarily on covered entities and business associates subject to the HIPAA rules. These HIPAA rules also can reasonably be applied today in connection with various forms of health care research, whether within the scope of the HIPAA rules or not. The health care sector will benefit from additional experts in this area as well as additional education and training on means of ensuring appropriate expert determinations. We encourage consideration by OSTP of means by which these HIPAA principles can be applied more broadly in other sectors. The government should evaluate how these principles can be applied in a broader setting outside of the health care industry. The government should both endorse the principles of the HIPAA de-identification approach and seek to apply it in other settings.

- Specific regulations or authorities that could be used, modified, or introduced to advance PETs; Specific laws that could be use, modified, or introduced to advance PETs; Existing best practices that are helpful for PETs adoption (Questions 4, 5 and 8)

The primary legal provisions related to the HIPAA de-identification standard are set forth in 45 C.F.R. § 164.514(a-b). HHS's most recent guidance for this standard is set forth in Department of Health and Human Service, Office for Civil Rights, "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule."[2] This standard is designed explicitly to facilitate

[2] *Id.*

and encourage the use of de-identification in the HIPAA environment, for the benefit of patients, the health care industry and the public at large.

Conclusion

At IQVIA, we have worked regularly with the HIPAA de-identification standard since it was developed by HHS. This standard has allowed IQVIA, its customers and its partners in the health care industry to utilize de-identified health care data for a broad range of medical research and public health purposes, as well as the overall facilitation of improved medical care in the United States and around the world. We encourage OSTP to endorse the framework of the HIPAA de-identification standard, and to explore means of expanding the utilization of this standard to a broader range of industries around the country.