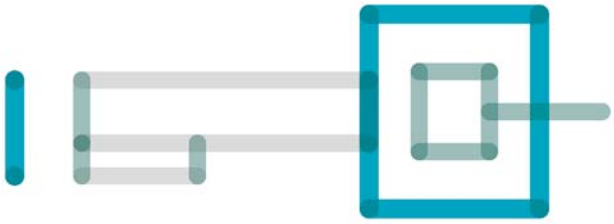

SOME FAQS ON HIPAA DE-IDENTIFICATION

Kirk J. Nahra[1]

Expert in privacy law and the Health Insurance Portability and Accountability Act, Kirk Nahra clarifies some of the most common queries regarding HIPAA compliant de-identification.

The broad public debate over "big data" and the increasing frequency of large scale security breaches involving sensitive personal data have highlighted the importance of de-identification as a means of permitting effective use of personal data while minimizing risks of privacy and security violations. While, in much of the world and in many industries, the discussion about de-identification involves important questions of how to define de-identified data and what this concept really means, the most precise definition of de-identification comes from the HIPAA Privacy Rule, covering the full range of protected health information developed and maintained by HIPAA covered entities. This HIPAA de-identification system – with its robust approach to defining de-identification of personal data – remains the "gold standard" for de-identification approaches in the legal system. Moreover, while there are various reports of "breaking" de-identified data collections, there have been no published reports detailing effective re-identification of data that has been de-identified consistent with the HIPAA standards.

With this background, it also is clear that there are important legal questions related to how the HIPAA de-identification principles work in practice, and ongoing discussions about whether the principles need to be changed or modified based on emerging technologies or evolving legal structures. This article reviews some of the most frequent issues that arise in this context.

A BRIEF REFRESHER

To put these FAQs in context, it is worth a brief refresher on the de-identification provisions of the HIPAA Privacy Rule.

The HIPAA rules created a set of standards for establishing when health care information was no longer "individually identifiable" - or

[1] The article is not legal advice, and should not be relied upon as legal advice. If you have questions about these legal issues, please consult your attorney.

would be considered "de-identified." Where information met the regulatory requirements for de-identification, health care information was considered "de-identified" by law, and therefore was no longer subject to the HIPAA restrictions on the uses and disclosure of individually identifiable information. Because the "individual" component of this information had been removed, this de-identified information then could be used and disclosed for a wide variety of purposes (including research and public health purposes as well as other commercial purposes), without creating meaningful privacy risks for any individuals. De-identified information is used widely for these secondary purposes, in the United States and across the world.

This HIPAA framework has existed since the HIPAA Privacy Rule went into effect in 2003. Pursuant to this framework, identifiable health care information is subject to HIPAA restrictions, and de-identified information can be used for additional purposes not subject to restriction under HIPAA that otherwise would be impermissible. (There are, of course, also good privacy reasons to use de-identified information even for otherwise permitted purposes, whether pursuant to the idea of "minimum necessary" or simply as a means of avoiding or reducing the risk of a privacy or security breach, but this approach is an issue of data "minimization" more than anything else).

The HIPAA Privacy Rule acknowledges and supports the benefits of these uses of de-identified information while, at the same time, recognizing that any material privacy interests have been eliminated through the de-identification process. HHS, in developing these standards, specifically wanted to ensure that "the Privacy Rule would not be a disincentive for covered entities to use or disclose de- identified information wherever possible." 67 Fed. Reg. 14776, 14799 (March 27, 2002).

The HIPAA De-identification standards were created by the original HIPAA Privacy Rule. Pursuant to that regulation, there are two basic methods by which Protected Health Information ("PHI") can be modified so that the PHI becomes "de-identified." The HIPAA rules provide that PHI is no longer regulated by HIPAA if the PHI has been "de-identified" consistent with the HIPAA Rules. The idea – from 45 C.F.R. § 164.514(a) – is that "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information."

Accordingly, under section 514 of the Privacy Rule, a covered entity or other entity "may determine that health information is not individually identifiable health information only if:

1. 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; or

2. (A specific list of) identifiers of the individual or relatives, employers, or household members of the individual, [is] removed.

Information is properly "de-identified," therefore, if the information meets either standard – the "expert determination" method or the "safe harbor" method.

DID THE HITECH LAW OR REGULATIONS CHANGE THESE PRINCIPLES?

The HITECH law modified various provisions of the HIPAA Privacy and Security Rules. These changes were not implemented until the issuance of the Omnibus Final Regulation in January of 2013, with compliance generally required by September 2013 for covered entities and business associates. The HITECH law made no changes to the de-identification standards set forth in the HIPAA Privacy Rule. The only mention of the de-identification principles in the HITECH statute requires that "Not later than 12 months after the date of the enactment of this title, the Secretary shall, in consultation with stakeholders, issue guidance on how best to implement the requirements for the de-identification of protected health information under section 164.514(b) of title 45, Code of Federal Regulations." The Omnibus Final Regulation similarly made no changes whatsoever to the substance of the de-identification standards of the HIPAA Privacy Rule.

There is little discussion of de-identification concepts in the Omnibus Final Regulation and its supporting commentary. One area where de-identification principles are discussed is in the context of the new provision prohibiting the sale of PHI in specified circumstances.

It is clear that the new HIPAA provision only prohibits the "sale of protected health information," which means the "disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information." If there is no "disclosure of protected health information," then there can be no "sale."

In addition, in its commentary to these changes, HHS makes clear that "[d]isclosures of health information that has been de-identified in accordance with the Privacy Rule at § 164.514(b)-(d) are not subject to the remuneration prohibition as such information is not protected health information under the Rule."

Accordingly, there is nothing in the HITECH law or the Omnibus final regulation that changes the core de-identification principles set forth in the HIPAA Privacy Rule.

DID HITECH CHANGE ANYTHING RELATED TO DE-IDENTIFICATION?

While the HITECH law (and the subsequent regulations) did not change the substance of the de-identification provisions, the law and regulations did make one important change in connection with the authority that is needed to de-identify information. It has been clear under the HIPAA rules (and remains clear today following HITECH) that a HIPAA covered entity has permission under the rules to de-identify information without the need for any patient authorization or other permission granted by a patient or another party.

Prior to the HITECH rules, there was some

ongoing debate about the authority of a business associate to de-identify information. It was clear under the HIPAA Privacy Rule that a covered entity could provide – in the business associate agreement or related service agreement – for a business associate to have the authority to de-identify consistent with the HIPAA standards. It also was clear that a business associate contract could preclude such de-identification, or impose specific limitations or conditions on this de-identification. The biggest "open question" under the original HIPAA Privacy Rule involved those business associate contracts (the substantial majority) that were silent on the question of a business associate's authority to de-identify information.

HITECH addressed this open question. It is now clear under the HIPAA rules that a business associate must be given specific authority under a business associate contract or service agreement to de-identify, with whatever conditions are attached by the covered entity. Without this permission, a business associate does not have the authority to de-identify information, even if the de-identification was conducted consistent with applicable law.

TO WHAT EXTENT ARE SECURITY CONTROLS A SUBSTITUTE FOR DE-IDENTIFICATION?

The HIPAA de-identification standard focuses on data elements, and an assessment of whether the remaining data elements leave a record that is "de-identified" consistent with the standard. One question that arises frequently is what the role of security controls is in connection with this expert determination, if any. Security controls do not, per se, have an impact on the specific data elements that are involved. However, it is clear that security controls provide an important additional protection for data, and that effective security controls play a role in preventing re-identification, whether from those with permission to utilize data or from outsiders.

Accordingly, the applicable security controls clearly are relevant to the overall determination by an expert as to whether information has been properly de-identified. Security controls are not, by themselves, sufficient. For example, it would not be consistent with the HIPAA rules to have a list of names and addresses of individuals and to say that this information is "de-identified" because it is always under a lock and key. However, when reviewing the value of data and the applicable data fields that remain once efforts have been made to de-identify the data, it is appropriate for an expert to consider overall information safeguards and security controls, as a component of the assessment of whether there is a small risk of re-identification of this data. The risk of re-identification is always smaller when there are effective security controls over the information. These controls will restrict the potential adversaries for the data, which in turn reduces the likely success of efforts to re-identify this data. Therefore, while effective security controls are an important element in all data protection contexts, there will always be a need for de-identification steps beyond safeguards for any true HIPAA de-identification.

WHAT ABOUT CONTRACTUAL CONTROLS?

Much like security controls, contractual restrictions are a useful and often significant element of protecting data so that a determination of de-identification can be made. Contractual limits protect data because they define how an appropriate recipient can use and disclose the data. However, also like security

controls, contractual controls are not sufficient by themselves to reach a de-identification decision. Contractual limits, if followed by the appropriate recipient, will mean that there are no intentional efforts to re-identify data. It reduces, but does not eliminate other risks (for example, of a security breach). The "best" de-identification programs will include robust data perturbation along with strong security controls and effective contractual limitations. De-identification can still be effective without the security or contractual controls (for example, in connection with a public release of data), but each factor will need to be weighed in an appropriate analysis.

CAN A BA DE-IDENTIFY DATA?

Business Associates are vendors who are retained by a covered entity to perform a specific service. In most situations, these business associates receive (and are permitted to receive) PHI to perform these services. Once a business associate agreement is executed, it is permissible for a covered entity to disclose PHI to its business associate.

In a limited range of situations, a covered entity may retain a business associate for the specific purpose of conducting de-identification. In these situations, the covered entity will provide PHI to the business associate, and will retain the business associate (pursuant to a business associate contract) to conduct a de-identification review and to de-identify the data. In this instance, the "service" being provided by the business associate is "de-identification." This step clearly is permitted by the HIPAA Rules.

In the more typical situation, where a business associate is retained to perform some service that involves PHI other than de-identification, the question remains whether the business associate is permitted to de-identify the data it receives from its covered entity customer. As discussed above, the rules on this have changed (or at least been clarified) as a result of the HITECH law. Now, business associates are permitted to de-identify information received from a covered entity only if the business associate has given this permission in the business associate agreement or related service agreement. Without this permission, the business associate does not have the authority to de-identify the information.

WHAT IF THE DE-IDENTIFICATION CONCLUSION IS WRONG?

If a de-identification review is conducted correctly, there will be only a small risk of re-identification of the data. It is important to remember, however, that even "compliant" de-identification is not perfect. Much like effective HIPAA security, where a risk of a breach remains (but is lessened considerably) even after the "reasonable and appropriate" steps have been taken to reduce security risks to acceptable levels, there is always a risk of re-identification, even after all the steps have been taken that are required by the HIPAA Rules.

Accordingly, entities involved with these issues should assess the risks related to de-identification and potential re-identification. While this assessment is important, it also is important not to over-react to these concerns. There has been no documented situation where a HIPAA de-identified data set has been re-identified. Where the appropriate steps are taken – and particularly where effective security and contractual controls are added – there is very little risk of re-identification.

So, companies should think about two kinds of issues in connection with de-identification. First, there is the risk that information has not in fact been properly de-identified. This is a realistic risk given that many companies do not properly understand the de-identification rules or have the knowledge or expertise to conduct an appropriate de-identification analysis. Therefore, any entity receiving such data should always be cognizant of these risks. Even if the data provided has been "de-identified," it always is appropriate to do a "reality check" on this data to confirm that the re-identification risk has been reduced to an acceptably low level. While (in theory) data that has been de-identified is no longer subject to the HIPAA rules, it is in the interest of all parties in the data chain to catch data that has not been properly de-identified and to prevent further disclosure or analysis of this data. Every entity in the chain also should be smart about how de-identification is conducted – do not engage in de-identification casually or without the appropriate expertise.

Similarly, even where the de-identification process has been conducted properly, some residual risk persists. Companies should always consider whether additional steps should be taken for protection of this data. Beyond the protection provided by "common sense" extra steps, this risk remains. There is no realistic history of "liability" in connection with de-identified data where the "small risk" actually occurs. Companies may choose not to engage in these activities, or may choose to attempt to define these responsibilities in contractual obligations, but keep in mind that there is a trade-off here. There is value (both economic and societal) in de-identified data. There also are important transactions costs from trying to allocate unknown risks or theoretical risks where there is no history. Accordingly, companies should be aware of these issues, and should evaluate their own appropriate response. That does not mean, however, that every potential situation can realistically be identified ahead of time or that all of these situations should be addressed in order to proceed in the de-identification process.

CONCLUSION

The issues discussed here are important and complicated, and will continue to be addressed in the years ahead. The increased recognition of the usefulness of de-identified data and the important opportunities provided by "big data" will work in combination to keep these issues in the forefront of our health care system and otherwise. Companies should remain vigilant on these issues, and should stay abreast of all meaningful developments.

ABOUT THE AUTHOR

Kirk J. Nahra is a Partner with Wiley Rein LLP in Washington, D.C. He represents a wide variety of companies on privacy, data security, cyber-security and security breach issues across the country and internationally. He chairs the firm's Privacy and Data Security practice. A long-time member of the Board of Directors of the International Association of Privacy Professionals and editor of IAPP's Privacy Advisor, he speaks and writes widely on a broad variety of privacy and data security issues. He can be reached at 202.719.7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.