PUBLICATION

Secondary Data Use Certification for Hospitals Now Available

Authors: Julie A. Kilgore
January 03, 2024

The value of data is on the minds of all industries right now, and health care is no different. The increased attention comes with the very significant shift in thinking, advanced by the attention to the advent of artificial intelligence. As an acknowledgment of the complexities, the Joint Commission established the Responsible Use of Health Data™ (RUHD) program, which became available to eligible hospitals (RUHD Certification) on January 1. RUHD Certification will provide an objective evaluation as to whether a hospital is committed to utilizing best practices in its secondary uses of data. While secondary uses of data may refer to a variety of potential data uses, the RUHD Certification's reliance on the Health Evolution Forum's *The Trust Framework for Accelerating Responsible Use of De-identified Data in Algorithm and Product Development* (Trust Framework) suggests the primary focus will be on the use of de-identified health data, which will also be the focus of this alert.

At first glance, you may be tempted to dismiss the RUHD Certification as not applicable to your organization given the limiting nature of the eligible applicants. However, the RUHD Certification will likely have downstream effects. For example, if an eligible hospital applying for RUHD Certification uses a third party for de-identification services, that third-party vendor should also expect to be asked to comply with data controls, limitations on use, de-identification practices, and other items that the applicant requires to obtain or maintain RUHD Certification. End users and other recipients of de-identified data should expect similar requirements.

The Health Insurance Portability and Accountability Act (HIPAA) and other related regulations and industry standards have long addressed the requirements and best practices for the use and disclosure of protected health information (PHI). However, while HIPAA details the standards and requirements for de-identifying PHI, HIPAA does not provide much guidance on how de-identified data can, or should, be used and disclosed. Beyond HIPAA's minimal support on the topic, the industry has also failed to adopt or consistently apply any given standards or best practices with respect to using and disclosing de-identified data. However, this RUHD Certification process is posed to bring changes to the industry.

In this alert, we'll discuss the RUHD Certification generally, the topics RUHD Certification covers specifically, and the likely impact of the RUHD Certification for, not only the eligible applicants for RUHD Certification, but also those applicants' vendors, customers, and end users of de-identified health data.

RUHD Certification: Overview

As of January 1, 2024, any hospital meeting the following requirements can voluntarily apply for RUHD Certification: (1) the hospital is in the U.S., operated by the U.S. government, or operated under a charter of the U.S. Congress; and (2) the hospital is compliant with applicable federal laws, including applicable Medicare Conditions of Participation.

RUHD Certification is intended to identify that the hospital has established and implemented policies and procedures to protect and promote responsible secondary uses of data. The RUHD Certification acknowledges the importance of secondary data uses but encourages organizations to participate in such use within a framework that mitigates risk and prioritizes patients' privacy. The RUHD Certification will review the

applicant's organization with respect to six topics, which are detailed more fully herein below – oversight structure, data de-identification, data controls, limitations on use, algorithm validation, and patient transparency.

RUHD Certification: Deep Dive on Topics Covered

Diving into the specifics of each area can provide insight as to what may be required to obtain RUHD Certification by applicants, and upon obtaining RUHD Certification, what requirements those applicants may flow down to their de-identification vendors, other vendors with access to such de-identified data, customers, and end users of de-identified data. As such, all potentially impacted organizations should begin reviewing and consider updating their practices in the following areas:

1. Oversight Structure. Effective data governance relies upon a foundational structure. Hospitals that do not currently maintain a framework or program (such as an Information Governance Committee) must establish a structure for the use of de-identified data. The development or updating of internal policies and procedures for the use of de-identified data will be foundational and will require input from a variety of stakeholders within the organization to ensure the data is used and disclosed in a manner that has been reviewed and approved by the organization. Considering the use and disclosure of de-identified data within an organization's overall data governance process will better enable an organization to meet the other requirements of the RUHD Certification. As noted below, de-identified data can be re-identified in certain situations, so it is important to document and understand at an oversight and decision-making position that this risk has been considered and mitigated. While not the focus of this alert, this will also enable an organization to ensure it has appropriate rights in its business associate agreements to use PHI for de-identification purposes and to address other regulatory or contractual requirements that may remain for de-identified data (e.g., confidentiality requirements, exchange of competitively sensitive information, or state privacy law impact on identifying information of individuals other than the subject of PHI).
2. Data De-Identification. The RUHD Certification will require organizations to de-identify PHI in accordance with HIPAA. HIPAA's de-identified data standard is 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. HIPAA only sets forth two methods for de-identifying PHI, the Expert Determination Method and the Safe Harbor Method. An organization must meet HIPAA's standards via one of the two de-identification methods, or the data remains PHI and subject to HIPAA requirements and limitations on use. The documentation regarding the method used, and the approval of such method will be important to maintain. Ensuring proper de-identification of data minimizes both patients' and organizations' risks related to the unauthorized use and disclosure of PHI.
3. Data Controls. The RUHD Certification will also require organizations to establish data controls to protect against unauthorized re-identification of de-identified data. Even when data has been de-identified in accordance with HIPAA, the data retains some risk of re-identification, so de-identification is only the first of many steps needed to ensure the data remains de-identified. Use or disclosure of re-identified data is a use or disclosure of PHI and subject to HIPAA requirements, so controls to prevent re-identification again minimize risks related to unauthorized use and disclosure of PHI. While the specific requirements for RUHD Certification are yet to be known, examples of controls that can protect against re-identification include creating administrative, technical, and physical controls to prohibit: (a) the combination or linking of de-identified data with identifiable data, (b) running of certain queries or application of certain filters to the de-identified data that may increase the likelihood of re-identification; (c) access by unauthorized users; and (d) export of de-identified data into an unprotected or third-party environment.

4. Limitations on Use. Organizations must also prohibit the misuse of de-identified data. Another way to minimize the risk of re-identification is to create contractual obligations that specify the permitted and prohibited uses and further disclosures of de-identified data and otherwise allow an organization to flow down certain requirements to third parties accessing or using de-identified data. Examples of terms that organizations may be required to input within its contracts to limit such use include: (a) detailed and narrowly scoped permitted use cases; (b) specific prohibitions on any other uses and/or particularly concerning uses, such as re-identification; (c) restrictions on further disclosures; (d) what, if any, derivate works are permitted, and usage rights related to the same; (e) security requirements; (f) audit rights related to use case compliance; (g) immediate termination rights for re-identification; (h) compliance with any expert statistician's certification requirements in determining the data has been and will remain de-identified; (i) return or destruction upon expiration or termination; and (j) restrictions on combining, linking, or storing with other data, particularly identifiable data.
5. Algorithm Validation. The RUHD Certification will require organizations to have processes to manage internally developed algorithms. De-identifying data does not protect, or exempt algorithms developed using such data from introducing biases, which may result in discriminatory output. Organizations developing algorithms must take steps to minimize the introduction of any biases. Examples of actions organizations may be asked to take include: (a) considering and identifying the elements contained within the data and where certain groups of the population may be over or underrepresented or biases are otherwise present; and (b) validating whether the algorithm, on an ongoing and consistent basis, addresses those biases to ensure the end product does not result in discrimination. Expertise in this area is important and third parties will likely need to be engaged.
6. Patient Transparency. Finally, the RUHD Certification will require hospitals to communicate with patients about secondary uses of de-identified data. As patients continue to become more aware and concerned about the privacy and security of their data in today's environment, organizations de-identifying and using patients' data need to be transparent about such use to build and maintain patients' trust. Hospitals should consider educating patients, potentially via notices of privacy practices, about the use cases that benefit health care and outcomes generally that would otherwise not be permitted with using PHI. Obtaining or otherwise complying with RUHD Certification may be a good first step in demonstrating to patients that a hospital has not only considered the importance of secondary usage rights but has also prioritized appropriate de-identification and use and disclosure of de-identified data to minimize privacy and security risks with respect to patient information.

RUHD Certification: Likely Impact

It is important to note that the Trust Framework was created by various industry stakeholders (payers, providers, life science companies, and others) with the hope that the principles would be applied by all industry participants, including both the producers and users of de-identified data. The adoption of the Trust Framework for the RUHD Certification may be the first of many applications of such standards and may not always be voluntary or limited to currently eligible hospitals.

Therefore, whether you will initially be eligible or plan to apply for RUHD Certification, the Trust Framework contains standards that all organizations involved in secondary data uses should consider adopting to: (1) build and maintain patient and industry trust; (2) minimize risks related to the unauthorized use and disclosure of PHI; and (3) ensure your secondary data use practices align with industry standards.

If you have any questions about secondary uses of data, de-identification practices, data governance, licensing de-identified data, or need additional information regarding this alert, please do not hesitate to contact Julie Kilgore, or any member of Baker Donelson'sData Protection, Privacy, and Cybersecurity or Health Law teams.