May 24-25, 2016

Hearing of the Subcommittee on Privacy, Confidentiality & Security
National Committee on Vital and Health Statistics

"De-Identification and the Health Insurance Portability and Accountability Act (HIPAA)"

Kimberly S. Gray
Chief Privacy Officer, Global
IMS Health

IMS Health is pleased to provide testimony before the Subcommittee on Privacy Confidentiality & Security of the National Committee on Vital and Health Statistics (NCVSH) related to "De-Identification and HIPAA".

BACKGROUND

IMS Health is a leading global information and technology services company, serving key healthcare organizations and decision makers around the world, including pharmaceutical, biotechnology, consumer health and medical device manufacturers, as well as distributors, providers, payers, government agencies, policymakers, researchers and others. IMS has pioneered practices to de-identify personal sensitive data, while serving a broad array of healthcare stakeholders, including the FDA and other agencies of the United States Department of Health and Human Services.

We are personal privacy and data protection advocates and leading experts in the collection, standardization, organization, structure, integration and analysis of health information.

We believe in the tremendous value of healthcare data for patients and the overall health care system, and believe that use and disclosure of this data, for research projects and other broad purposes, can be conducted in ways that are beneficial to patients in improving their health outcomes and the overall health care system without sacrificing patient privacy interests.

Our intent today is to help raise awareness and understanding of HIPAA's robust guidance for de-identification and the important role that de-identification plays in protecting patient privacy, while advancing data-driven health care improvements. We believe that (1) the HIPAA de-identification approach provides strong, effective protection for individual privacy interests while still permitting beneficial uses of de-identified data that help patients and the health care system and that (2) this approach, as written into the HIPAA Privacy Rule, evolves with business changes and new technology, such that no changes are needed to this framework.

HIPAA AND DE-IDENTIFICATION

The HIPAA Privacy Rule contemplates a spectrum of information ranging from fully identified to fully anonymous, and it catalogues information into categories of identifiable (protected

Kimberly S. Gray
Chief Privacy Officer, Global
Tel: 484-567-6045
Email: kgray@us.imshealth.com
IMS Health
One IMS Drive
Plymouth Meeting, PA 19462, USA
www.imshealth.com

health information or PHI), limited data sets (where most direct identifiers are removed) and de-identified data (where there is a very low risk of re-identification).

Although the HIPAA de-identification framework is not the only de-identification approach that is available (in the US and elsewhere), it provides a useful model for analysis and discussion because it is more detailed and comprehensive than other applicable approaches. It is the gold standard for de-identification and adapts well to changing data sources and changing technology; in fact, the HIPAA framework incorporates technological change as a component of its overall analysis. It strives to balance the need to protect individuals' identities with the need to allow de-identified databases to be useful.

When the Department of Health and Human Services (HHS) was considering the HIPAA Privacy Rule, HHS saw the need for an overall balance between privacy interests and the overall operation of the healthcare system. The overall "use and disclosure" principles of HIPAA reflect this balance. The de-identification principles reflect another component of this balance – the protection of privacy interests through appropriate de-identification while still permitting uses and disclosures of data that benefit patients and the healthcare system. De-identification is a vital tool and means to engage in privacy protective data stewardship when conducting data analytics that are fundamental to improving patient care.

When evaluating the alternative, release of only anonymous information (i.e. zero risk approaches versus very small risk approaches), HHS officials made clear that a "stronger" de-identification standard would provide no more than a marginal boost in privacy protections with the much higher costs of reducing beneficial uses and disclosures of this de-identified information. Further, any "zero risk" standard precluded many laudable and valuable uses of data 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 re-identification.

While much has changed in the healthcare landscape since HIPAA's inception, including greater availability and use of data, concerns about the sufficiency of the HIPAA de-identification methodologies are largely unfounded. HIPAA de-identification methodologies are holistic, risk-based and readily adapt to changes.

To meet the overall standard set forth in the HIPAA Privacy Rule (particularly using the "expert determination" method, effective de-identification is a combination of removing, generalizing and disguising patient identifiers, imposing privacy and security safeguards (i.e., administrative, technical and physical safeguards, including contractual limitations), and a mindfulness as to the value of research data and appropriate protection of privacy.

VERY LOW RISK OF RE-IDENTIFICATION: Policies and Practices

In order to determine that data is properly de-identified (i.e., very low risk of re-identification), several steps should be followed:

- First, re-identification risk thresholds should be determined, considering the context of the data, data recipients, potential re-identification attacks and controls. If the measured risk is below the threshold, then the data will be considered to be de-identified.
- Next, there must be a way to objectively measure the risk of re-identification in a repeatable and objective manner; therefore, metrics must be defined that are consistent with the plausible attacks that have been identified and the nature of the data.
- Then, direct identifiers are removed, and indirect identifiers are evaluated (and possibly removed); special attention should be paid to dates and geo-locators.

Kimberly S. Gray
Chief Privacy Officer, Global

Tel: 484-567-6045
email: kgray@us.imshealth.com

IMS Health
One IMS Drive
Plymouth Meeting, PA 19462, USA
www.imshealth.com

- The methodology must also consider potential adversaries interest in re-identifying the data.
- At this point the organization will transform the data to de-identify it (e.g., via suppression, pseudonymization, generalization, perturbation, substitution, elimination of small cell counts, k-anonymity, etc.
- Lastly, auditable controls to manage residual risk must be put in place, and data utility must be considered.

This protocol works as a standard means of de-identification. Although "big data" may complicate the risk evaluation, there is nothing about it that requires changes to the HIPAA framework, because the very factors that make data "big data" are accounted for in the HIPAA de-identification framework.

BENEFICIAL USES OF DATA

The HIPAA Privacy Rule anticipates the beneficial uses of de-identified data to advance healthcare in such forms as expanding medical research and improving public health. Healthcare data that has been properly de-identified can be used for such purposes as:

- rapidly detecting disease outbreaks,
- detecting geographic tendencies,
- performing quality and outcomes research analyses,
- reducing medical errors and improving patient safety,
- reducing healthcare disparities,
- providing provider quality of care information,
- carrying out comparative effectiveness research,
- health economics and outcomes research,
- monitoring adherence to therapies, etc.

Reports issued by the IMS Health Institute for Healthcare Informatics provide examples of many of these uses of de-identified data fundamental to improving patient care.

HITRUST

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of the broad adoption of health information systems and exchanges. HITRUST established a certifiable common security framework (CSF) to be used by all organizations creating, accessing, storing or exchanging personal health and financial information. The CSF harmonizes existing standards and regulations such as HIPAA/HITECH, PCI, COBIT, NIST and FTC.

The CSF was modified in 2015 to include a de-identification framework. HITRUST looked at guidance related to de-identification from various countries and agencies around the world, yet its framework is very reliant upon the HIPAA de-identification framework, as this was found to be the most robust and helpful.

We include a short slide deck to highlight certain aspects of the HITRUST De-Identification Framework that are relevant to the discussion points of this hearing.

We also include a link to further explain the benefits of the HITRUST de-identification framework. https://hitrustalliance.net/de-identification/

Kimberly S. Gray
Chief Privacy Officer, Global

Tel: 484-567-6045
email: kgray@us.imshealth.com

IMS Health
One IMS Drive
Plymouth Meeting, PA 19462, USA
www.imshealth.com

IN SUMMARY

De-identification - whether through the HIPAA model or otherwise - is a useful tool in protecting individual privacy interests, while at the same time enhancing innovation and the improved use of health and other personal information for important public and private purposes. In many situations, de-identified data can be leveraged to provide the same analytical value as using PHI, while fully embracing HIPAA's minimum necessary concept and appropriately protecting individual privacy interests. Through more than a decade of practice under the HIPAA Privacy Rule, the HIPAA de-identification standard has resulted in exactly the goal set out by HHS in drafting this portion of the Privacy Rule: effective protection of individual privacy interests while still permitting a broad range of uses and disclosures of this de-identified information that benefits patient healthcare interests and the effective operation of the overall health care system.

Thank you for this opportunity to provide testimony and to answer questions.

Kimberly S. Gray, J.D., CIPP/US
Chief Privacy Officer, Global
IMS Health

Kimberly S. Gray
Chief Privacy Officer, Global

Tel: 484-567-6045
email: kgray@us.imshealth.com

IMS Health
One IMS Drive
Plymouth Meeting, PA 19462, USA
www.imshealth.com

Hearing of the Subcommittee on Privacy, Confidentiality & Security National Committee on Vital and Health Statistics

De-Identification and HIPAA

Usefulness of the HITRUST De-Identification Framework

Kimberly S. Gray, J.D., CIPP/US

Chief Privacy Officer, Global; IMS Health

May 25, 2016

imshealth™
INTELLIGENCE APPLIED.

HITRUST De-ID Framework

Defines categories of health information

Evaluates de-identification methodologies

Addresses expert qualifications

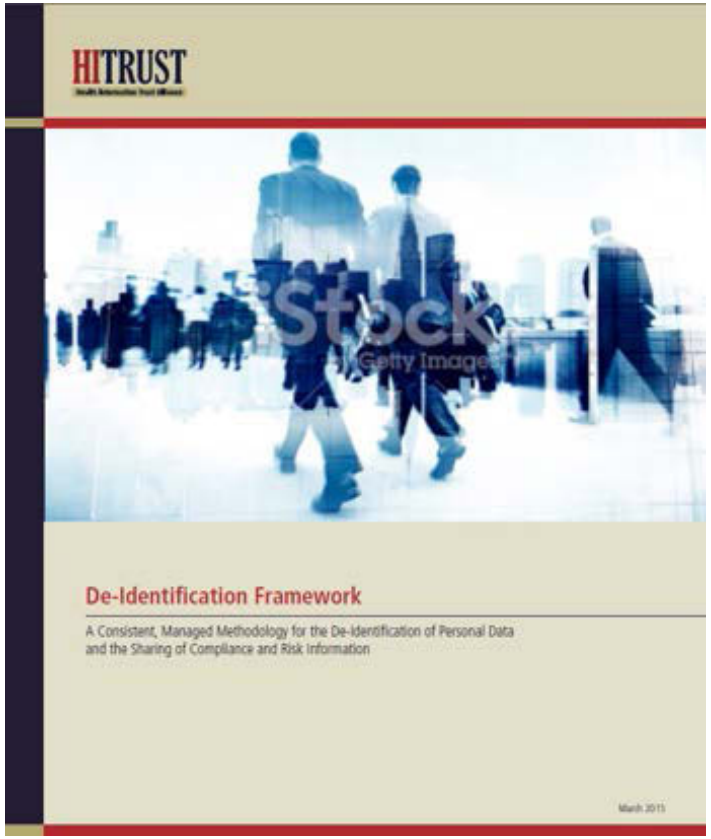
Measures re-identification risks

Maps to the HITRUST Common Security Framework (CSF)

Training program underway

Assessments

Regulatory support



imshealth™

Recommendations for a De-ID program

- Taking into account the size, complexity, and capabilities of your company and the amount of de-identification activities, establish a de-identification program, including:
  - Governance
  - Documentation
  - Explicit identification of the data custodian and recipients
  - External or independent scrutiny
  - Explicit agreement by recipients that re-identification will not be attempted.

Recommendations for a De-ID program

- Establish a de-identification methodology, that takes into account:
  - Re-Identification risk thresholds
  - Measurement of actual re-identification risks
  - Identification and management of direct identifiers and quasi-identifiers
  - Identification of plausible adversaries and attacks
  - Identification of specific data transformation methods and how they reduce the risks
  - Process and template for the implementation of re-identification risk assessment and de-identification
  - Mitigating controls to manage residual risk
  - Data utility

Thank you for this opportunity.