



Data Protection Accountability and the Appropriate Use of De-Identified Data

February 2010

BACKGROUND

For more than 50 years, IMS Health has been a leading provider of information services to healthcare stakeholders and a pioneer in the development and use of safeguards to protect patient privacy. IMS Health operates in more than 100 countries and provides valuable insights to commercial organizations, researchers, non-profit organizations, government organizations and others that improve healthcare quality and operations. IMS Health collects information, using extensive privacy protections and safeguards, from a wide variety of sources, including pharmacies, physicians, hospitals, insurers, health maintenance organizations, pharmacy benefits managers, wholesalers, manufacturers and other healthcare stakeholders.

IMS Health believes that individual privacy can and must be preserved and protected while health information is used responsibly to improve healthcare delivery. IMS Health-pioneered privacy protections and safeguards rely on collection and use of de-identified patient information.¹ IMS Health believes de-identified patient information, combined with wise and responsible use, advances worldwide medicine and improves healthcare quality and value for patients. De-identification, combined with appropriate administrative safeguards, assures patient privacy and information security.


This paper advocates for data protection accountability and the appropriate and responsible use of de-identified data as an effective and trustworthy means to protect patient privacy.

IMPROVED DATA PROTECTION: De-identified health data is one key mechanism

An essential goal of data protection is that of preventing physical, financial and social harm to individuals and society as a result of inaccurate, incomplete, lost, stolen or otherwise compromised personal information.

While it might be instructive to focus on remediation of harms as a means of gaining consumer and patient involvement, it is prudent to attempt to prevent the harm from occurring in the first place by taking reasonable steps to protect personal information, bearing in mind the sensitivity of the data, the likelihood

¹ “De-identified patient information”: 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; it is not individually identifiable health information. 45 CFR 164.514.



that its compromise could result in harm, and the significance and severity of any resulting harm.

Because properly protected de-identified information is not linked to a particular individual, de-identification supports this objective. For much of our work, risk of harm is greatly reduced when the information has been stripped of identifiers.

DE-IDENTIFICATION, ENCRYPTION AND SECURITY SAFEGUARDS: Creation of 'patient-anonymous' health data sets

Requiring patient consent for every data collection or use would cripple the flow of health data and impede quality research, healthcare improvement efforts and basic healthcare operations. It would also be a burden to those older patients afflicted with chronic or rare diseases who would be enlisted for a disproportional number of research projects. A more rational method, and one advanced by our nation's health information privacy laws, is to undertake considerable efforts to ensure patient-identifiable information is not disclosed inappropriately and that data analysis and research is conducted with de-identified health information whenever possible.


IMS Health collects prescription data from thousands of United States pharmacies. The data is de-identified at these pharmacies before it is transferred to IMS Health, using both trusted third parties and multiple layers of encryption. IMS Health never has access to any encryption keys used in the process and no single person or entity (including IMS Health) can unlock these encryption keys to access the patient identity from the raw data.

As responsible data stewards, IMS Health further protects de-identified data through technical, physical and administrative security safeguards. This critical layer of protection ensures that IMS Health data are used solely for the intended purpose, physically secured, and accessed only by those trained in data protection and with a defined need.

IMS Health reports, analyses and services are produced from databases that contain no patient identifiable information, and these reports themselves contain no patient identifiable information.

IMPROVED HEALTHCARE: Free-flow of de-identified data key to its use

The vast majority of healthcare quality and outcomes research analysis does not require patient-identifiable information, but can be accomplished with de-identified data. Quality assurance and quality improvement, treatment practices and protocols, patient safety, reduction of medical errors and healthcare cost management all benefit from the availability and use of de-identified data.



As our nation pursues healthcare delivery improvements, other organizations could follow the lead of IMS Health and use de-identified data for their operations.

At IMS Health, using de-identified data we support many activities and research around the globe, including:

- Track antibiotic resistance patterns geographically.
- Perform healthcare cost effectiveness analyses.
- Track prescription antiviral treatment variations and how they affect morbidity and mortality rates (e.g., H1N1).
- Correlate prescription patterns with outcomes and treatment patterns.
 - all without knowing the identity of the patient.

Additional healthcare operations that could use de-identified data to advance healthcare include:

- Improve care and case management initiatives using risk category analysis.
- Stratify into risk categories for wellness profiles.
- Map member data to providers to determine provider network access needs by geography/locale and by specialty.
- Examine volume and cost of particular procedures by providers to enhance quality through incentives and better reimbursement systems based on geography and provider type.
- Larger data-sharing initiatives and projects can be designed and move ahead without privacy concerns.
- Plan-based utilization reports that do not violate privacy concerns or raise fears of discrimination.

ACCOUNTABILITY: Underlying principle to advance and promote responsible data stewardship

Creating a regulatory scheme around de-identified data is not only unnecessary, but may impede access to data. Impeding access to data stifles innovation and is at odds with improving patient outcomes, decreasing medical errors, advancing utilization of health information technology, and myriad other goals of healthcare reform.

Making it difficult to use de-identified information increases privacy risks. Unless it is easy to use de-identified data, healthcare stakeholders will resort to using patient-identifiable information for their operations, leading to an increased risk of patient-identifiable data compromise with potential risk of harm.

A better approach is adoption of the well-established principle of data protection known as accountability, which is found in the laws of the United States, Canada, the European Union and its member states, in OECD Guidelines and emerging privacy governance globally.



An accountability-based approach to data governance focuses on setting data protection goals based on legal requirements, public policy, self-regulation and best practices. An accountable organization then uses its discretion to determine the most appropriate ways to meet these goals. Because this approach is adaptable, an accountable organization can meet consumer demands, business needs and changing technology without impediment.

Accountable organizations take responsibility for the data they safeguard by ensuring they have appropriate systems, policies and procedures, training, monitoring and oversight in place. They follow generally accepted industry best practices, and they agree to be answerable for their data handling practices.

At IMS Health, we are committed to following this principle and we promise to handle our data assets with care as our way of doing business. We understand that if we break this promise, we are answerable and subject to penalty.