Information Governance and DEID

- Lucy Doyle, VP Data Protection, Strategy and Secure Information Management
- Karen Smith, Sr. Dir., Global Privacy Office

Disclaimer

Disclaimer: The contents of this presentation are the experiences, opinions, and/or views of the authors and do not represent an official position of their employer nor is it being offered as legal guidance.

Overview

- HIPAA De-identification: Safe Harbor and Expert Determination Methods
- Evaluating the risks of re-identification
- Understanding practical application of a de-identification program, including technical, organizational and legal controls.
**What is de-identification?**

- Removal of Protected Health Information (PHI) so that the risk of re-identification of an individual who is the subject of the information is ‘very small’, as required by the HIPAA Privacy Rule (45 CFR 164.514).
- There are two methods to de-identify data:
  1. **Safe Harbor** method: Removal of all 18 PHI identifiers and any other identifying information, or,
  2. **Expert Determination** method: Expert review by a person with appropriate knowledge and skill who uses generally accepted scientific principles and methods to determine that the risk of re-identification of an individual is very small.
- With both methods, de-identification is to be maintained in upstream and downstream uses of the data.

**Safe Harbor Method**

Requires removal of 18 identifiers of an individual or of relatives, employers, or household members of the individual:

<table>
<thead>
<tr>
<th>Name</th>
<th>Social Security Number</th>
<th>URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographic subdivisions smaller than a state</td>
<td>Health plan beneficiary number</td>
<td>Device identifiers / Serial number</td>
</tr>
<tr>
<td>All elements of dates (except year) directly related to an individual (e.g., DOB, admission date)</td>
<td>Medical record number</td>
<td>Biometric identifiers including finger and voice prints</td>
</tr>
<tr>
<td>Telephone number</td>
<td>Account number</td>
<td>Full face photo and comparable images</td>
</tr>
<tr>
<td>Fax number</td>
<td>Certificate / License numbers</td>
<td>IP address numbers</td>
</tr>
<tr>
<td>E-mail address</td>
<td>Vehicle identifiers / Serial number</td>
<td>Any other unique identifying number, characteristic or code</td>
</tr>
</tbody>
</table>

**Expert Determination Method**

- Certification by expert that risk of re-identification is ‘very small’
- Expert must be sufficiently competent to document and defend the statistical and scientific methods used to evaluate risk and the results of the analysis
- Office of Civil Rights (“OCR”) provides guidance but does not set a numerical threshold for risk

Applies generally accepted statistical and scientific principles and methods to PHI to meet HIPAA standard for de-identification
Myths and Misconceptions

Ø Aggregation and summarization = de-identification

Ø Once Expert determination approves as de-identified, the data set can be reused for different intended uses.

Ø If I cannot re-identify, no one can and the risk is small thus de-identified.

Determining Risk

Ø Collaboration with Stakeholders
Ø Use Case Definition and Clarity
Ø Identify PHI – Know the data, including indirect identifiers and other unique characteristics and codes
Ø Effective Use of De-identification Methodologies – Clear methods of de-identification (Safe Harbor method is deceptively simple)
Ø Risk Determination by an Expert
Ø Minimum Necessary Standard has been Applied
Ø Appropriate Data Sharing Agreements

Disclosure Limiting Techniques Examples

<table>
<thead>
<tr>
<th>Perturbation Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removal</td>
<td>Removal of sensitive data from data set or record.</td>
</tr>
<tr>
<td>Masking</td>
<td>Replace original values in a data set with realistic but fake data.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Values can be aggregated to provide better de-identification</td>
</tr>
<tr>
<td>Suppression</td>
<td>Removal or masking of value. Can be done to data element or entire record.</td>
</tr>
<tr>
<td>Other</td>
<td>Business rules to be applied</td>
</tr>
</tbody>
</table>
Technical, Organizational & Legal Controls

ØTechnical
§ Controlled Access
§ Portability Controls (e.g. Thumb Drives, VPN Access etc.)
§ Encryption
§ Access Management
§ System Audits
ØOrganizational
§ HIPAA Privacy and Security Training
§ Access Exception Process
§ Sensitive Data Review Process
§ Vendor Assurance Program
ØLegal
§ Data Rights
§ Patient Authorization
§ Documentation Template
§ Data Strategy

Authors

Lucy Doyle:
Ph.D. in Human Services/Healthcare Administration with focused research in the area of data confidentiality involving privacy and security controls and de-identification of data. Has more than 16 years of experience in data handling, data aggregation, data benchmarking, and de-identification of data. Prior positions include MTS Chief Privacy and Data Security Officer, Per-Se VP Privacy and Compliance, NDCHealth Chief Privacy Officer. Designated as McKesson Distinguished Technologist 2014.

Karen Smith:
Is responsible for the development and implementation of privacy and data protection program strategy. Routinely provides guidance around data protection standards, and data de-identification/anonymization methodologies to support commercialize data products. Previously, Ms. Smith was an associate with Gust Rosenfield, PLC, and Director, Billing Compliance, Wal-Mart Stores, Inc. Ms. Smith holds a juris doctorate and has spoken on privacy and security and related healthcare compliance topics.