MCKESSON

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.

MCKESSON

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.

MCKESSON

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.

MCKESSON

Safe Harbor Method

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

Name	Social Security Number	URLs
Geographic subdivisions smaller than a state	Health plan beneficiary number	Device identifiers / Serial number
All elements of dates (except year) directly related to an individual (e.g., DOB, admission date)	Medical record number	Biometric identifiers including finger and voice prints
Telephone number	Account number	Full face photo and comparable images
Fax number	Certificate / License numbers	IP address numbers

Covered Entity must not have "actual knowledge" that the information could be used alone or in combination with other information to identify an individual who is the subject of the information

MCKESSON

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

MCKESSON

Myths and Misconceptions

ØAggregation and summarization = de-identification

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

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

MCKESSON

Determining Risk

ØCollaboration with Stakeholders

ØUse Case Definition and Clarity

ØIdentify PHI – Know the data, including indirect identifiers and other unique characteristics and codes

ØEffective Use of De-identification Methodologies – Clear methods of de-identification (Safe Harbor method is deceptively simple)

ØRisk Determination by an Expert

ØMinimum Necessary Standard has been Applied

ØAppropriate Data Sharing Agreements

MCKESSON

Disclosure Limiting Techniques Examples

Perturbation Method	Description
Removal	Removal of sensitive data from data set or record.
Masking	Replace original values in a data set with realistic but fake data.
Aggregation	Values can be aggregated to provide better de-identification
Suppression	Removal or masking of value. Can be done to data element or entire record.
Other	Business rules to be applied

MCKESSON

Technical, Organizational & Legal Controls

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

MCKESSON

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 Rosenfeld, 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.