MEDICAL DEVICE
DATA ANONYMIZATION & RISK METHODOLOGY
Training Course

BOOK NOW

June 19, 2019: 11am to 5pm
June 20, 2019: 9am to 5pm
W Hotel – City Center
172 West Adams Street, Chicago, Illinois, 60603-3604

Technical Requirements:

Laptop with permission to access remote desktop

Course Summary:

Demonstrating the full value of medical devices through measurable patient outcomes, personalized treatment insights, and R&D initiatives requires careful consideration (beyond legal compliance under HIPAA, CCPA and GDPR). It's a balancing act that's essential in the face of growing public scrutiny, the changing legal landscape and the threat of market disruptors and insurgents.

The central question is how to use data in a way that protects individual privacy, while ensuring that it remains of sufficient quality for useful and meaningful analytics. Our consistent answer is data de-identification.

The best way to responsibly share protected health information is by applying a risk-based de-identification methodology. Privacy Analytics is pleased to offer training that teaches medical device companies how to safely and securely share their data assets while minimizing the risk of re-identification.

This risk-based methodology is consistent with best practices for anonymization. It has been applied for more than a decade globally to facilitate the sharing and secondary use of data. The course structure consists of in-person lectures and hands-on exercises to allow participants to understand the steps and decisions that need to be made when implementing pseudonymization and anonymization methods.

This event is right for you if…

- You're looking to gain the highest possible data utility at the lowest possible risk;
- You're assessing anonymization techniques that best align to your business needs;
- Your organization uses a risk-based approach and you want to enable more team members;
- You currently, or plan to, de-identify medical images;
  Your organization has challenges regarding data privacy.

Course Outline

Module 1 – Legal Considerations
A discussion of the legal bases for using and disclosing information for secondary purposes under HIPAA, CCPA, and GDPR, and when each can be applied.

Module 2 – Concepts and Definitions
An overview of known re-identification attacks, analysis of different data release models and classification of identifiers.

Module 3 – Risk Measurement Concepts
An introduction to equivalence classes, and discussion of various risk types & metrics, and their relevance to various anonymization use cases.

Module 4 – Analysis of Context Risk
Descriptions of different types of attacks and how to evaluate the risk of them re-identifying data subjects. This module also covers choosing an acceptable threshold for the risk of re-identification based on the characteristics of the dataset.

Module 5 – Data Transformation Methods
Methods to mask direct identifiers and de-identify quasi-identifiers.

Module 6 – Risk Management and Reporting
Determining if the risk is below an acceptable threshold. Creating a report and documenting that the risk of re-identification is very small.

About the Moderator

Luk Arbuckle - Chief Methodologist, Privacy Analytics

Advising healthcare enterprises topping the *Fortune* 500, Luk Arbuckle has co-authored books, scholarly journal articles and patents on re-identification risk and de-identification. He brings a decade of experience in the field of anonymization, and is co-author of *Anonymizing Health Data: Case Studies and Methods to Get You Started* (O'Reilly Media, 2013/2014).

Mr. Arbuckle is currently Chief Methodologist at Privacy Analytics. He was formerly Director of Technology Analysis at the Office of the Privacy Commissioner of Canada and Research Manager and Data Scientist at the Children's hospital of Eastern Ontario (CHEO) Research Institute in Ottawa. He holds multiple graduate degrees and was awarded numerous scholarships and bursaries.