A methodology for achieving successful results with healthcare IT by balancing risk management with an optimal implementation approach.
AGENDA

INTRODUCTION

WHAT IS GDPR & WHO IS AFFECTED?

REQUIREMENTS FOR COMPLIANCE

ENFORCEMENT & FINES

SUMMARY OF RECOMMENDATIONS

QUESTIONS?

ABOUT THE PRESENTERS

BRIAN SELFridge | PARTNER, MEDITOLOGY SERVICES
Brian leads Meditology’s IT Risk Management practice and has advised hundreds of healthcare organizations across the country. Prior to Meditology, Brian was the CISO of AtlantiCare, a large integrated healthcare provider located in New Jersey. Brian has over 16 years of experience in healthcare security and privacy. He is a frequent presenter and expert speaker on an array of healthcare security topics. As an industry-thought leader he advises several federal agencies including: OCR, HHS, and ONC. Brian’s combination of both consulting experience with hands-on operational security leadership sets him apart as one of the healthcare industry’s leading experts on data risk management and compliance strategies.

NADIA FAHIM-KOSTER | PARTNER, MEDITOLOGY SERVICES
Nadia Fahim-Koster is an industry thought-leader in managing healthcare privacy and security programs. She leads the Information Technology Risk Management practice for Meditology Services, the #1 Cybersecurity Advisory Services firm ranked in the 2019 Best in KLAS Software and Services Report. She has more than 15 years operational experience as a former CISO and CPO with many large hospital/physician networks, academic medical centers worldwide. Nadia is a sought-after consultant and presenter on privacy, security and compliance programs including addressing all requirements for HIPAA/HITECH, GDPR as well as PCI standards.
2019 BEST IN KLAS

- Second year Meditology has been recognized by KLAS for excellence in client service
- 30,000 interviews conducted with InfoSec and IT leaders at health systems and health plans across the country
- KLAS ranking directly reflects how we are viewed for excellence in client service

WHAT IS GDPR & WHO IS AFFECTED?
WHAT IS GDPR?

• Enacted by the European Union
• Effective May 25, 2018
• Designed to give EU residents more control over their personal data
• GDPR is “consumer-centric” (i.e. follow the data)
• Controls for how data is collected, stored, transmitted and destroyed (collectively, “how data is processed”)
• Successor program to the EU privacy rules introduced in 1990’s
• Above and beyond HIPAA

8 MONTHS OF GDPR

• Effective date: May 25, 2018
• More than 59,000 data breach notifications
• 91 fines
  • Exposure of personal data
  • Failing to protect employee passwords
  • Operating an unauthorized CCTV system that partially surveilled a public sidewalk
• Regulators are just getting started
WHAT IS IN SCOPE FOR GDPR?

- Personal data means any information relating to EU residents
- Much more than PHI -- PII, PCI, PHI & much more

WHO IS AFFECTED?

- GDPR APPLIES:
  - If you employ EU citizens, you must protect their information
  - If your business has a physical presence in EU
  - If you have clients in the EU (contractors and vendors)
  - If you market to EU patients and customers
  - If you maintain EU citizen data
- Size of the organization does not matter
Source for this is from OCR directly at HCCA conference earlier this year, will send you content, will need to cite it.

Brian Selfridge, 8/9/2018
WHICH HEALTHCARE ENTITIES ARE AFFECTED?

**Covered Entities (Providers & Payers)**

- If you market to EU patients
- If you have physical locations in the EU
- GDPR does NOT apply if:
  - You see patients in the US that are visiting from the EU
  - You are storing data for household or personal use (like friends in the EU and their contact info, processing has to be part of an “enterprise”).

**Business Associates**

- If you have clients and customers in the EU
- If you market to EU customers and clients
- If you offer a solution (e.g. cloud or SaaS solutions) to EU companies or companies that have EU citizen data
- If you possess the names, photos, email addresses, medical information, and financial information of any EU resident
- If you are a Pharmaceutical or Medical Device company with products in the EU

REQUIREMENTS FOR COMPLIANCE
SEVEN PRINCIPLES

1. Lawful, fair and transparent processing
2. Purpose limitation
3. Data minimization
4. Accurate and up-to-date processing
5. Limitation of storage
6. Confidential and secure
7. Accountability and liability

REQUIREMENTS FOR COMPLIANCE

- Implement "reasonable data protection measures" for EU personal data:
  - Article 32 gives examples of security measures, but does not dictate specific controls
  - Healthcare entities can leverage US frameworks like HITRUST & NIST
  - HITRUST being updated to include GDPR controls
  - Hacking and Pen Tests: "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing"
  - "Pseudonymization & encryption of personal data"
- Data Protection Impact Assessments (think HIPAA risk analysis)
BS1 Source for this is from OCR directly at HCCA conference earlier this year, will send you content, will need to cite it
Brian Selfridge, 8/9/2018
SOME OF THE MORE IMPACTFUL CONTROLS FOR U.S. ORGANIZATIONS INCLUDE:

- **CONSENT** - Must be "freely given, specific, informed, and unambiguous," and a person must be allowed to withdraw consent at any time. There are additional consent requirements when the person is a child under the age of 16.

- **PRIVACY NOTICES** - Provide a detailed list of all EU personal data that will be processed, the business’ contact information, the purposes for which the personal data will be collected, whether the business intends to transfer the personal data to another party, and any other information related to the individual’s rights regarding the personal data and how those rights can be exercised.

- **BREACH NOTIFICATION** - Far more rigorous than U.S. breach notification laws. Time frame is 72 hours. Provide specific details of the breach such as the nature of it and the approximate number of data subjects affected. Must notify affected parties.

- **DATA PROTECTION OFFICER** - Must appoint a Data Protection Officer (DPO). One estimate shows 78,000 new data protection officer jobs being created.

- **RIGHTS IN PERSONAL DATA** - EU citizens have the Right to Access and Right to be Forgotten (deletion of records). Data Portability also requires EU citizens to be able to receive a copy of their data.

- **PERSONAL DATA SECURITY** - Businesses are required to implement the "appropriate level of security" for the personal data they process, including protection against loss, destruction, damage, or unauthorized access. Businesses will also have to maintain records of their personal data processing activities.

- **CROSS-BORDER DATA TRANSFER** - Permissible transfer of personal data from the EU to non-EU countries. "Cross-Border Data Transfer" requirements are complex, extremely onerous, country specific, and include certain Codes of Conduct and certifications that should be reviewed and understood prior to transferring any EU resident’s personal data.
WHO ENFORCES GDPR?

Supervisory Authorities (SAs)
- Conduct audits
- Review certifications
- Issue warnings should it appear a GDPR violation may occur
- Order a processor or controller to comply with GDPR
- Impose limitations, and even bans, on processing
- Impose administrative fines
- Suspend data flows it deems as non-compliant

EU member states appoint an SA
- Which SA you deal with may depend on the specific individuals or companies involved in a breach or enforcement activity
- The European Data Protection Board coordinates enforcement activities
HOW ARE FINES CALCULATED AND LEVIED?

Information Commissioner’s Office (ICO) issues the fines:

- Factors under article 83:
  - The nature, gravity and duration of the infringement
  - Whether the infringement was intentional or negligent
  - Whether the organization took steps to mitigate damage
  - Technical and organizational measures that had been implemented by the organization prior to the breach
  - The degree of cooperation with the regulator
  - The types of personal data involved

- Maximum fine is up to 4% of annual global turnover or €20 million ($24,690,800 US) [whichever is greater]

- Fines can range between 2% to 4% and are calculated considering the factors outlined above

ENFORCEMENT EXAMPLES

- Barreiro Montijo hospital was fined €400,000
- Excessive access provisioned to patient data in the hospital’s EMR
- 985 users had access rights of a medical doctor, although only 296 physicians were employed
- Access control failure; policy, procedure, and implementation
Source for this is from OCR directly at HCCA conference earlier this year, will send you content, will need to cite it.

Brian Selfridge, 8/9/2018
ENFORCEMENT EXAMPLES (cont.)

- France fined Google nearly $57 million
- Lack of transparency
  - “Users are not able to fully understand the extent of the processing operations carried out by Google.”
- No valid consent
  - “The information on processing operations for the ads personalization is diluted in several documents and does not enable the user to be aware of their extent”

WHAT IS PRIVACY SHIELD?

Privacy Shield is a framework and program for providing transparency for protecting EU personal data.

- Established in February of 2016
- Over 2,400 companies currently participate
- Companies must publicly self-certify to the Department of Commerce that they are compliant with the framework
- Voluntary process
- GDPR requirements are much more onerous than Privacy Shield (i.e. If you participate in Privacy Shield, you have more work to do to comply with GDPR)
- U.S. is not considered a trustworthy destination by EU, so you likely need Privacy Shield in order to receive EU personal data going forward
Source for this is from OCR directly at HCCA conference earlier this year, will send you content, will need to cite it.
Brian Selfridge, 8/9/2018
SUMMARY OF RECOMMENDATIONS

• Review the scope considerations with legal counsel and determine if GDPR is in scope
• If in scope:
  • Conduct a GDPR readiness assessment
  • Develop policies and procedures
  • Appoint a Data Protection Officer (could be same as CISO or CPO, if applicable)
  • Inventory locations and scenarios where EU personal data is processed
  • Perform a Data Protection Impact Analysis
  • Review consent processes and update accordingly
  • Update data breach and record retention policies and procedures to address more stringent requirements
  • Update contracts with third parties if applicable
  • Align remediation and corrective actions with other related HIPAA and risk analysis activities
THANK YOU

Meditology Services is a professional services company with an exclusive focus on healthcare IT. Our reputation for client service excellence is based on the quality of our work products combined with the professionalism, approach, and innovative solutions we bring to our engagements.

BRIAN.SELFRIDGE
@MEDITOLOGYSERVICES.COM

NADIA.FAHIM-KOSTER
@MEDITOLOGYSERVICES.COM