HIPAA and GDPR

Joe Dickinson - Smith Anderson
Tim Opsitnick - TCDI
April 16, 2018

GDPR - Key Elements

• What?
  ○ To process information you need demonstrate Legal Basis/Transparency/Fairness

• Who? Potentially any company worldwide that offers products or services to or monitors EU residents
  ○ Risk Areas
    - Sales
    - HR
    - Job Applicants
General Data Protection Regulation

- What?
  - Valid Consent
  - DPO?
  - PIA
  - Data Breach Notification
  - Data Subject Rights
    - Right to Erasure (to be forgotten)
    - Rights of access
    - Right to Rectification
    - Right to Restriction
  - Data Controllers and Data Processors
    - Controllers only engage processors with “sufficient guarantees”
    - Technical and organizational measures
  - Privacy by Design

- Pseudonymization
- Encryption
- Ensure ongoing confidentiality, integrity, availability - Sound familiar? HIPAA?
- Resilience of processing systems and services
- Process for regularly testing, assessing and evaluating effectiveness of technical and organizational measures for ensuring security of processing
General Data Protection Regulation

• Broad application
• Greater Risk
• Need to Assess
• Document

GDPR - Key Healthcare Concerns

• HIPAA and GDPR Definitions may differ
• GDPR - Legality, transparency and fairness
• HIPAA - required and permitted uses/disclosures
• Patient rights v. Data subject rights
• Pseudonymization v. anonymized v. de-identified
GDPR and HIPAA

• Who Is Covered?
• Patient Consent/Authorization
• Breach Notification - 72 hours
• Business Associates/Onward Transfer
• When? Store data, transfer data, receive data, access data, for any purpose (especially if international business is involved) - including IP, HR, Marketing, Investment, Financial Reporting, Risk Management, Regulatory

Compliance Implications
Why this Topic Isn’t Fun

• Too many laws and regulations
  - Confusing and Constantly Changing
  - Overwhelming/Frustrating
• It doesn’t apply to me/Not likely to have an issue
  - But required to assess and document
• Inhibit/prohibit business growth and operations
  - Too many corporate resources required for compliance
• Positions Business Organizations to be a victim twice

Focus on Underlying Priorities

• Organizational Culture
• Top-down responsibility and involvement
• Demonstrated priority on privacy and security of data
• Have a program - be proactive
• Are you doing what you say you will do?
• Remember that GDPR impacts far more businesses than commonly understood
Focus on Common Legal Themes

- Risk Assessments/Risk Analysis (Privacy Impact Assessment PIA)
- Designated Person of Responsibility (DPO, PO, SO)
- Training
- Sanctions
- Regularly Updated Policies/Procedures
- Regular audits
- Incident Response Plan
- Access Management/Logging
- Document, Document, Document

Have a Compliance Program

- Some Key Elements
- Address, in writing, Individual Rights-
  - Are they prioritized?
  - Clearly identified?
- Organizational Obligations
  - Accountability
  - Address both Privacy and Security?
  - Is it a living, breathing program?
  - Regular Review and Update - policies, procedures, training, etc.
  - Understand data flow and risks
  - IRP for Breaches/Incidents
    - Anticipate and prevent
    - Respond
Final Thought...

- Have a compliance program, no matter how basic
- Document what you do to show steps taken to comply

Questions?

- Thank you