108 - Navigating Data Protection Requirements and Participant Rights in Research Studies

June 12, 2023

Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

Agenda

Introduction

Questions and Complexities

Data Protection Principles

Regulatory and Compliance Considerations

Case Study

Navigating Data Protection and Rights

Questions

Introduction

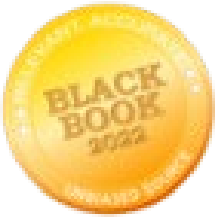
Andrew Mahler, JD, CIPP/US, CHPC, CHRC, CHC

VP, Privacy and Compliance Services

- Responsible for services and teams that support diverse clients in managing compliance and regulatory risks, including initiatives associated with HIPAA; federal, state, and global data protection; healthcare compliance; research compliance; and others
- Former Investigator for the U.S. Department of Health and Human Services, Office for Civil Rights (OCR)
- Served in Chief Privacy Officer and Research Integrity Officer roles
- Healthcare law course developer and instructor
- Published and presented on topics including health law, healthcare compliance, data privacy and HIPAA, research compliance, and risk management

Clearwater Overview

- Award-winning cybersecurity and compliance consulting, outsourced managed services, and software focused on the healthcare and DIB ecosystem
- 500+ customers across major hospital systems, large physician practice groups, digital health, medtech, payors and defense contractors
- 200+ colleagues with 100+ expert cybersecurity & privacy consultants in U.S.
- Tech-enabled 24x7x365 Security Operations Center with Managed Detection & Response (MDR) Services
- Proprietary IRM|Pro® SaaS-based software platform enables efficient identification and management of cybersecurity and compliance risks
- Certified HITRUST Assessor & first approved Certified Third-Party Assessment Organization in the Cybersecurity Maturity Model Certification (CMMC) program
- Rapidly growing and profitable portfolio company of Altaris Capital Partners, a healthcare PE firm with more than $5B under management



Healthcare's Top-Rated Security Advisors

Healthcare's Top-Rated Compliance & Risk Management Solution *6th Consecutive Year*

Won the 2023 Cybersecurity Excellence Awards for Best Cybersecurity Solutions Consolidator Company and Best Security Risk Management Solution for Healthcare.

Clearwater

Our Areas of Expertise

We combine people, process and technology to deliver better, easier and more cost-effective solutions through consulting or outsourced managed services.

Cybersecurity Program Leadership & Execution

vCISO, Maturity Assessments, Strategy, Transformation ClearAdvantage® Program

Risk Analysis & Risk Management

Risk Analysis, Response, Monitoring, 3rd Party Risk

ClearConfidence® Program

Compliance & Privacy

Advisory, Audit, Certification

HIPAA, OCR, GDRP, CCPA, HITRUST, PCI, CMMC, SOC 2, EPCS

Managed Security Services / SOC

MDR, 24x7x365, Threat Detection, Vulnerability/Firewall Mgmt.

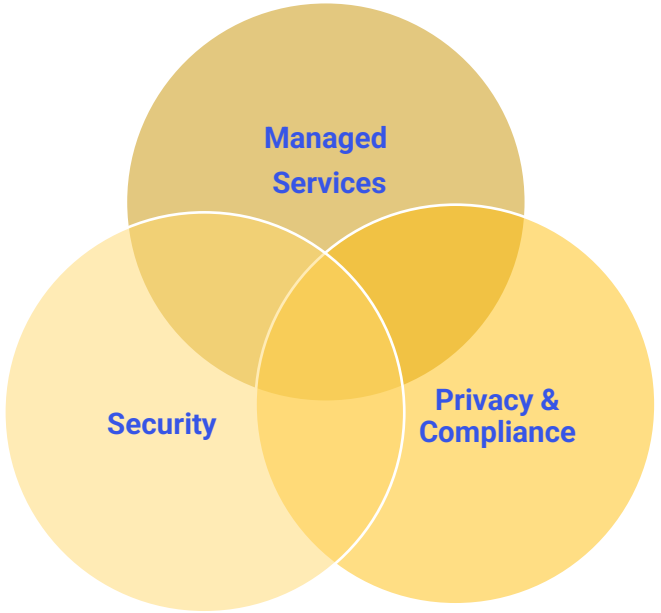
Security Eng. / Technical Security Services

Cloud Security, Technical Testing, Security Engineering, Remediation, Med Device & IoT Security

Emergency Operations / Incident Response

BIA, BCP, DRP, IR Planning, IR Exercises, IR Support

We Address Healthcare Market Segment-Specific Needs



Health IT | Hospitals | PPMG | Medtech

Clearwater

Extensive Experience in the Hospital and Health System Sector

Questions and Complexities

Questions

- Do you know who is operationally responsible within your organization for data protection policies and procedures?
- Do you know what data protection rules apply to your projects/office?
- Does your organization provide data protection support to individual studies?
- Does your organization's training and education include data protection considerations beyond HIPAA?
- Have you participated in a data flow or data mapping initiative?
- What data protection framework(s) does your organization use?
- Is your organization monitoring access to information about patients/participants?

Complexities

- Covered entities, business associates, and hybrid entities
- PHI and identifiable health information/research information
- Authorization or consent (or both)
- Privacy and security incidents
- Individual rights
- Roles and role-based access
- Data warehouses
- De-identification
- Minimum necessary vs. all data
- *Others?*

Data Protection Principles

Fair Information Practice Principles (FIPPs)

- Widely accepted in the United States and internationally as a general principles in privacy frameworks
- Provide a framework for organizations to handle personal information in a fair, transparent, and accountable manner
- Serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies
- Designed to build public trust in the privacy practices of organizations and to help organizations avoid tangible costs and intangible damages from privacy incidents

FIPPS

1. The Collection Limitation Principle
2. The Data Quality Principle
3. The Purpose Specification Principle
4. The Use Limitation Principle
5. The Security Safeguards Principle
6. The Openness Principle
7. The Individual Participation Principle
8. The Accountability Principle

FIPPS

1. The Collection Limitation Principle
   - There should be limits to the collection of personal data *(information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer)* and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
2. The Data Quality Principle
   - Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date
3. The Purpose Specification Principle
   - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose

FIPPS

4. The Use Limitation Principle
   - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject, or by the authority of law
5. The Security Safeguards Principle
   - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data
6. The Openness Principle
   - There should be a general policy of openness about developments, practices and policies with respect to personal data
7. The Individual Participation Principle
   - An individual should generally have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them
8. The Accountability Principle
   - A data controller *(the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data)* should be accountable for complying with measures which give effect to the principles stated above

Privacy By Design

- *A framework and approach that aims to proactively embed privacy and data protection principles into the design and architecture of various systems, rather than addressing privacy as an afterthought or add-on measure*
  - Privacy is embedded in the design - *FIPPS are considered at every stage of development*
  - Proactive not reactive, preventative not remedial
  - Privacy is a default setting
  - Full functionality
  - End-to-end security – *full lifecycle protection*
  - Visibility and transparency – *keep it open*
  - User control and empowerment – *keep it user-centric*
  - Respect for user privacy

Regulatory and Compliance Background

Regulatory and Compliance Background

- Common Rule
- HIPAA
- GDPR
- State law requirements (ex. CPRA)
- Other international requirements (ex. PIPEDA)
  - Canadian federal law that governs the collection, use, and disclosure of personal information by private sector organizations in Canada
- Site/IRB requirements
- Contracts

Regulatory and Compliance Background

- HIPAA
  - Applies to covered entities and business associates
  - Applies to PHI/ePHI
  - Requires authorization in many situations
  - Provides individual rights
  - Requires administrative, technical, and physical controls
  - Requires breach notification and reporting
  - The federal “floor” for protection of health information

Regulatory and Compliance Background

- GDPR
  - Applies to organizations that have an establishment within the EU, regardless of where data processing takes place
  - Applies to organizations outside the EU if they process personal data of EU residents in connection with offering goods or services to EU residents or monitoring their behavior within the EU
- CCPA
  - Have an annual gross revenue of $25 million or more
  - Buy, sell, or share the personal information of 50,000 or more consumers, households, or devices
  - Derive 50% or more of their annual revenue from selling consumers' personal information

Case Study

Case Study

- *A large-scale clinical research project conducted by a renowned medical institution, researching the efficacy of a novel treatment for a rare disease. The study involved hundreds of participants across multiple sites, and their sensitive personal and medical information was collected and stored as part of the research process.*
- What were the challenges?

Case Study Challenges

- Regulatory and compliance requirements
- Data security: maintaining consistent data security measures across all centers is crucial to protect participant data from unauthorized access or breaches
- Participant consent: ensuring that participants provide informed consent and are fully aware of their rights regarding their personal data throughout the study
- Data sharing: facilitating secure data sharing among collaborating research institutions while adhering to data protection regulations and maintaining participant privacy

Succeeding at the Intersection of Data Protection and Research Activities

Navigating Data Protection and Rights - 10 Considerations

1. Understand data protection regulations – *familiarize yourself with relevant data protection regulations*
2. Consider the purpose(s) – *and the minimum necessary rule*
3. Implement a robust Consent/Authorization process – *transparency and opportunities for participant to ask questions*
4. Consider individual/participant rights
5. Consider anonymization, de-identification and pseudonymization of data first – *when required/possible*

Navigating Data Protection and Rights - 10 Considerations

6. Secure data storage and transmission – *provide support to studies*
7. Data retention and disposal – *who/what is monitoring?*
8. Monitor and manage access – *proactive and reactive*
9. Effective training, education, resources – *consider tailoring for studies using/disclosing regulated/sensitive data*
10. Ongoing compliance reviews/audits – *the processes and the data*

Questions?

Thank you!

andrew.mahler@clearwatersecurity.com

Clearwater

Healthcare – Secure, Compliant, Resilient

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their missions.