CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Five Years Later

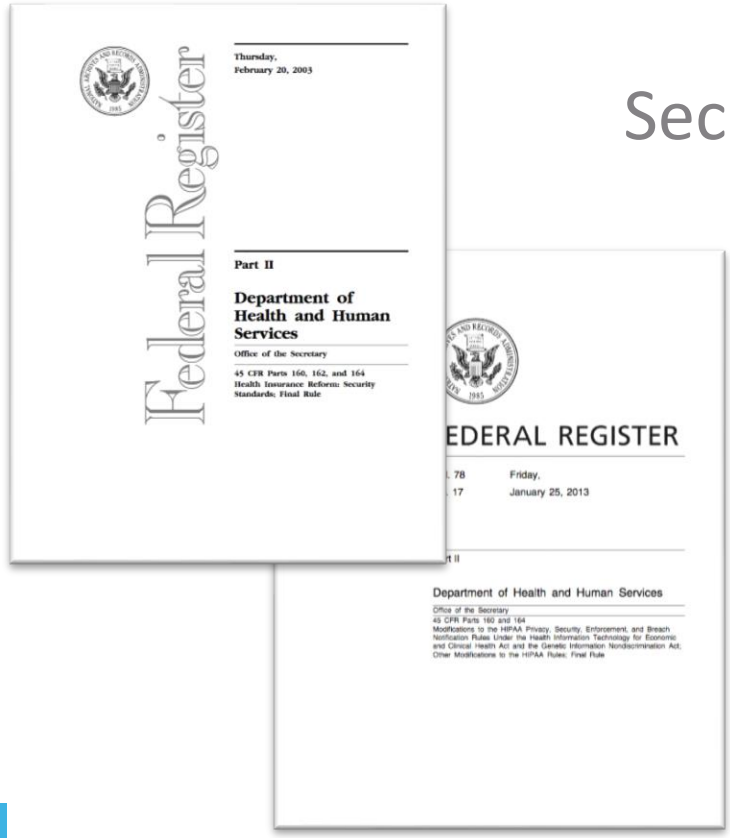
Is it time for Healthcare to Look at the NIST Cybersecurity Framework to Support HIPAA Compliance?

HIPAA Summit 2020
Mini-Summit XII
March 3, 2020

29th National HIPAA Summit

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

HIPAA Security Rule



Security Standards – Final Rule 2003

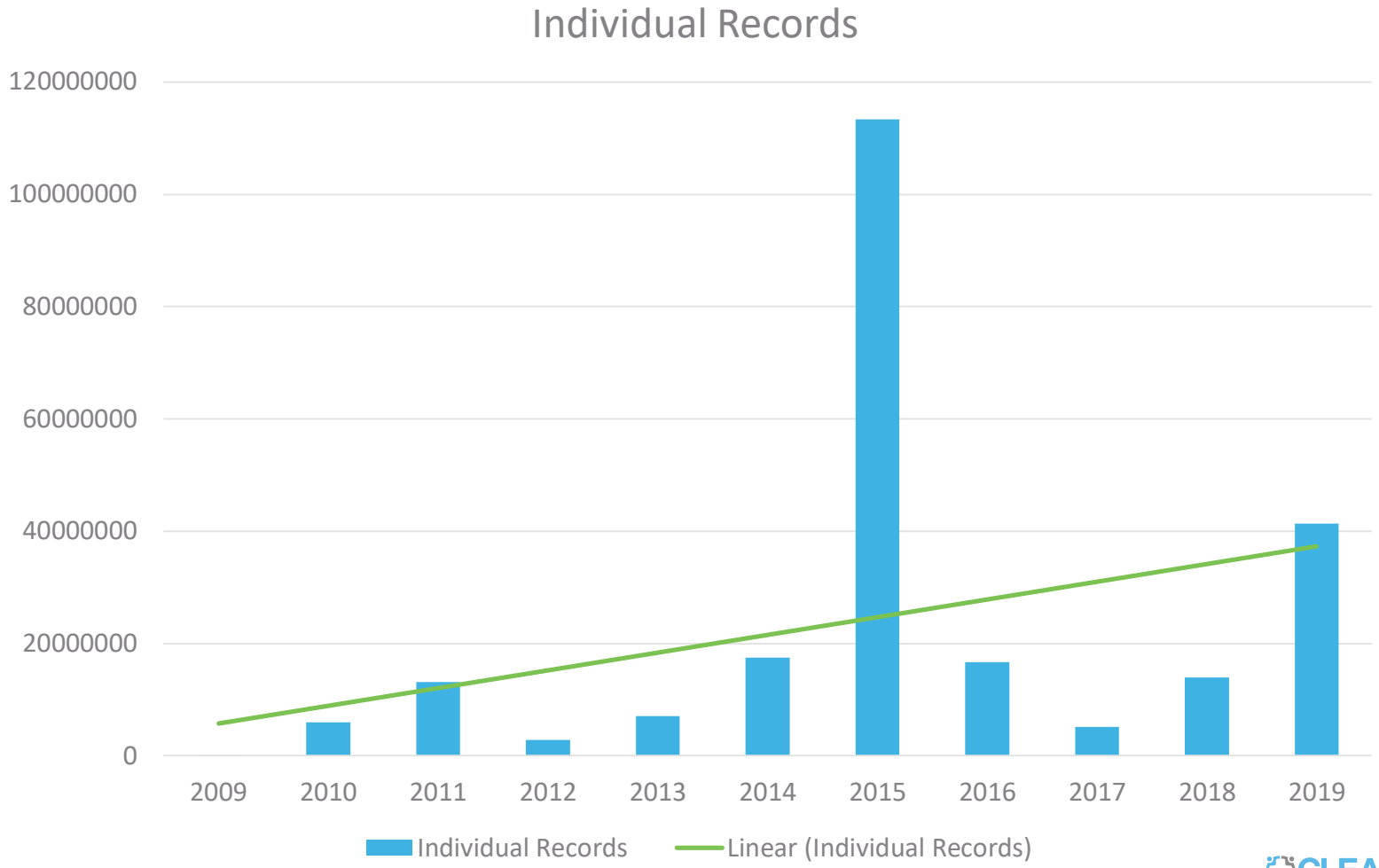
Omnibus– Final Rule 2013

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

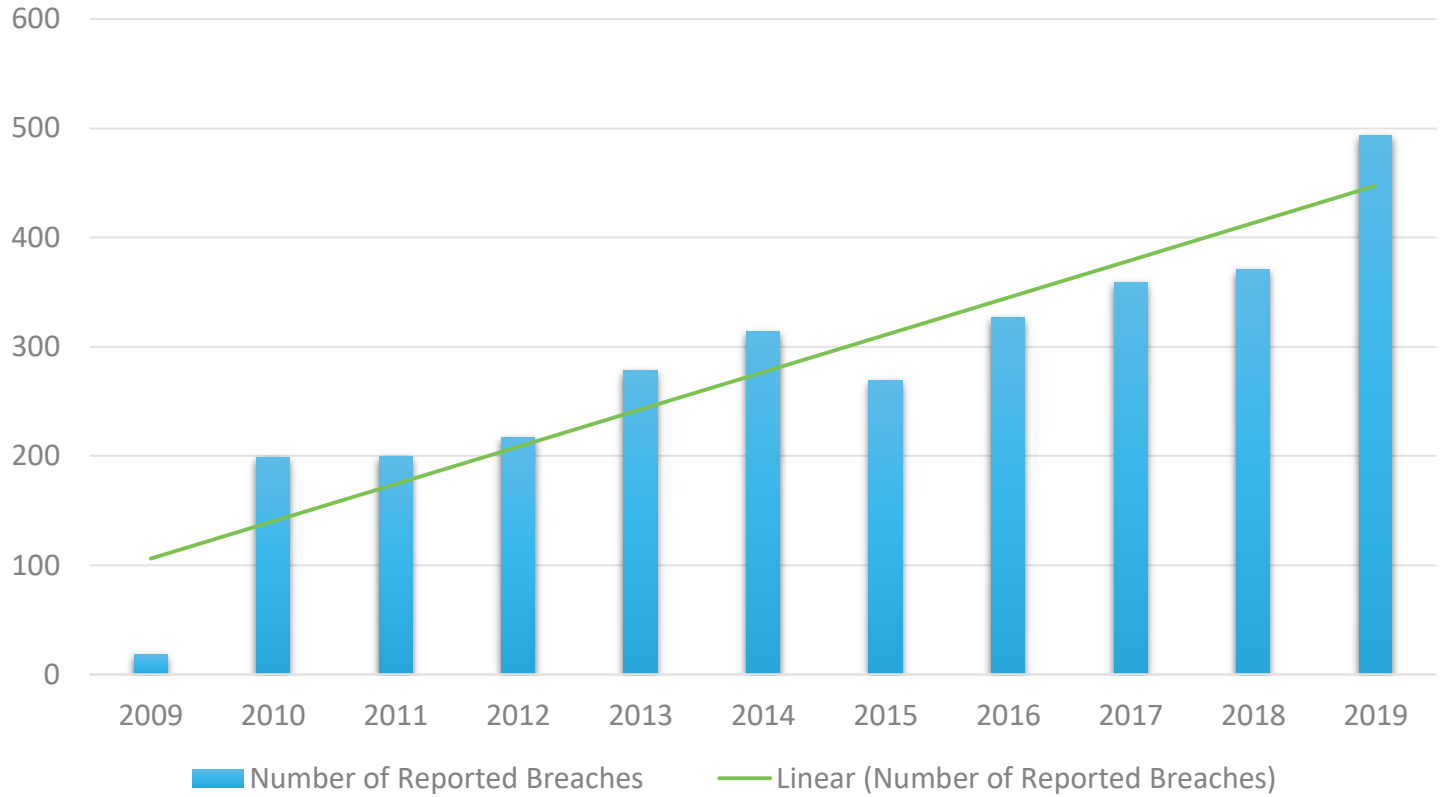
HIPAA Security Rule General Requirements

1) Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit
2) Identify and protect against reasonably anticipated threats to the security or integrity of the information
3) Protect against reasonably anticipated, impermissible uses or disclosures; and
4) Ensure compliance by their workforce

How are we doing?



Number of Reported Breaches



CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Why is this happening?

Increasing complexity of IT.

Increasing attack surface.

Increasing sophistication of adversaries.

Increasing compliance requirements distracting from security.

Insufficient resources (staff/budget).

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Explanation or Excuse?

How do we get to a place where we achieve both the requirements of the HIPAA Security Rule and its Objectives?

It’s a controls-based world.

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Industry Control Frameworks

- ISO
- NIST 800-53
- CIS

Compliance Driven Control Frameworks

- HIPAA
- PCI
- 800-171
- State Requirements (ex NY SHIELD)

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Control Frameworks to Comply with Control Frameworks

- HITRUST
- Secure Control Framework
- Custom Organization Frameworks

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT


Frameworks are intended to help us bring order to chaos and complexity but instead we have added more complexity.


This guy keeps winning.

What is the alternative?

Once upon a time at a Big 4.

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Somewhere along the way we forgot our destination.

NIST Cybersecurity Framework

Credit: N. Hanacek/NIST

Version 1.0 2014

Version 1.1 2018

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Cybersecurity Framework Example

Function	Category	Subcategory
IDENTIFY (ID)	**Risk Assessment(ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.**	ID.RA-1:Asset vulnerabilities are identified and documented
		ID.RA-2:Cyber threat intelligence is received from information sharing forums and sources
		ID.RA-3:Threats, both internal and external, are identified and documented
		ID.RA-4:Potential business impacts and likelihoods are identified
		ID.RA-5:Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6: Risk responses are identified and prioritized

NIST Cybersecurity Framework v1.1

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Adoption of Cybersecurity Framework

Control Category	Control Expectations are Not Defined or Implemented	Control Expectations are Defined	Control Expectations are Implemented	Control Expectations are Repeated or Reported (Managed)	Control Expectations are Regularly Reviewed and Updated	Control Expectations Audited	Average Measurement Score for Category
Security Objectives within Project Management			✓	✓			2.0
Development, Enhancement, and Acquisition of Systems		✓			✓		2.0
Software and System Maintenance Agreements	✓						0.0
End-of-life and Obsolete Systems		✓	✓	✓	✓		4.0
Change Control		✓	✓	✓	✓	✓	5.0
Reviews and Tests of Critical Changes		✓	✓	✓	✓		4.0
Reviews of Failed Changes		✓	✓	✓	✓		4.0
Asset Data Destruction		✓	✓	✓	✓		4.0
Disposition of Hardware		✓	✓	✓			3.0
Network Inventory Practices		✓	✓		✓		3.0
Network Asset Movement		✓			✓		2.0
Network Equipment Maintenance			✓				1.0

Target Profile

–

Control	Control Expectations are Not Defined or Implemented	Control Expectations are Defined	Control Expectations are Implemented	Control Expectations are Repeated or Reported (Managed)	Control Expectations are Regularly Reviewed and Updated	Control Expectations Audited	Average Measurement Score for Category
Security Objectives within Project Management				✓			1.0
Development, Enhancement, and Acquisition of Systems		✓			✓		2.0
Software and System Maintenance Agreements	✓						0.0
End-of-life and Obsolete Systems		✓			✓		2.0
Change Control		✓	✓	✓	✓	✓	5.0
Reviews and Tests of Critical Changes		✓			✓	✓	3.0
Reviews of Failed Changes		✓	✓	✓	✓	✓	5.0
Asset Data Destruction		✓	✓	✓	✓		4.0
Disposition of Hardware			✓				1.0
Network Inventory Practices		✓			✓		2.0
Network Asset Movement		✓			✓		2.0
Network Equipment Maintenance			✓				1.0
Procedures and Schedules for Network Maintenance	✓						0.0
Server Inventory Management		✓	✓	✓	✓	✓	5.0
Backup of Servers Prior to Movement			✓				1.0
Authority and Identification of Individuals for Server Movement		✓			✓		2.0

Current Profile

=

Action Plan

1. Implement Control
2. Implement Control

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Principle Based Policy Governance

Principles	The five principles relay the intent of the Board and defines organizational information security expectations.
Policy Statements	The twenty-three policy statements are defined and accepted at the leadership level of the organization and are aligned to meet the intent of the cybersecurity principles.
Directives	Directives align to the NIST-CSF Subcategory Level. Directives further define expectations or Policy Statements and are aligned directly to established cybersecurity framework standards.
Security Standards	Security standards are based on pre-defined standards from the NIST CSF and it's referenced controls from CIS, ISO 27002, and ISO 27005; however, these may be customized for organizationally-based controls.
Procedures and Guidelines	Procedures describe security related processes, activities, and methods for implementing and maintaining requirements defined within the organization's Security Standards. Guidelines provide guidance and pragmatic advice about fulfilling the requirements established by the organization's Security Standards. Although the guidance and advice are discretionary, the underlying requirements are usually mandatory.

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

Putting this together gives us something unique. The whole organization focused on the benefits and outcomes of our program rather than the controls.

Nothing is Free.

When implemented we have a cybersecurity program with objectives linked to corporate strategy. Those objectives are understood from the Board level down. Requests for investment are linked to the objectives and the risk of not making them is well understood.

Focused on achieving the benefits of our cybersecurity program, we can comply with the HIPAA Security Rule but most importantly achieve its objectives.

Thank You & Questions

Jon Moore
Jon.Moore@ClearwaterCompliance.com
615.656.4299
www.clearwatercompliance.com

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

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.

CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT

www.ClearwaterCompliance.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-compliance-llc/

Twitter | @clearwaterhipaa