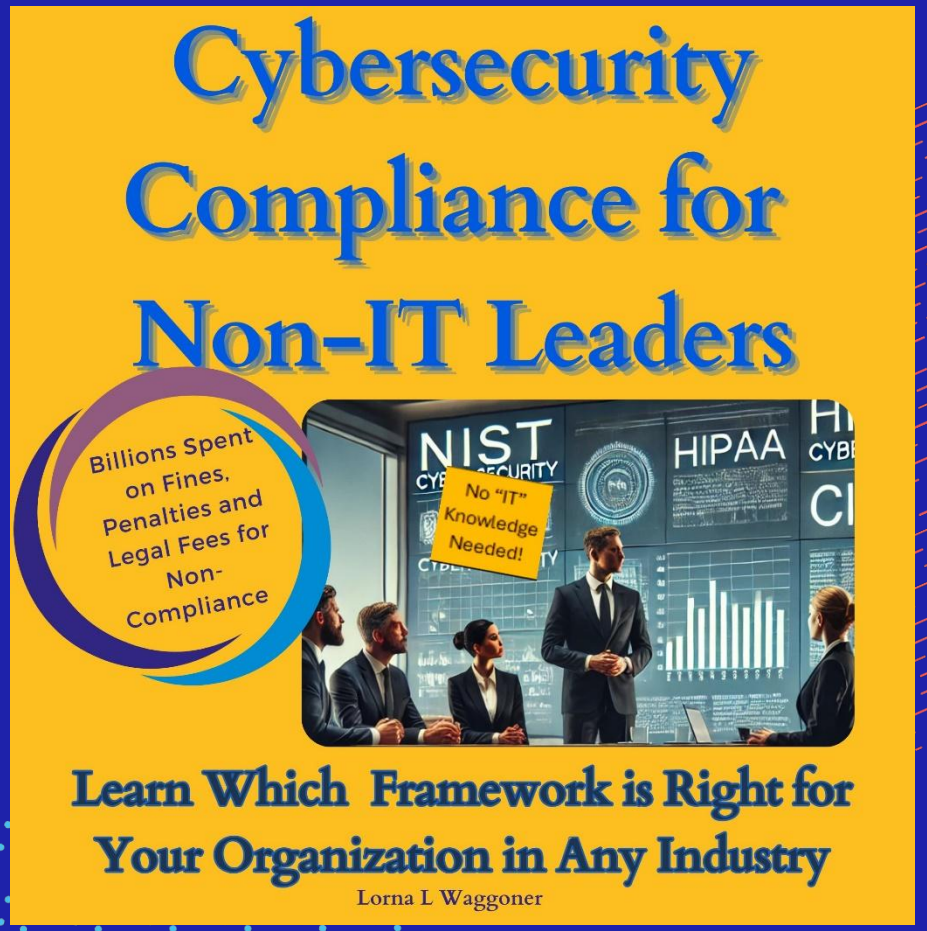
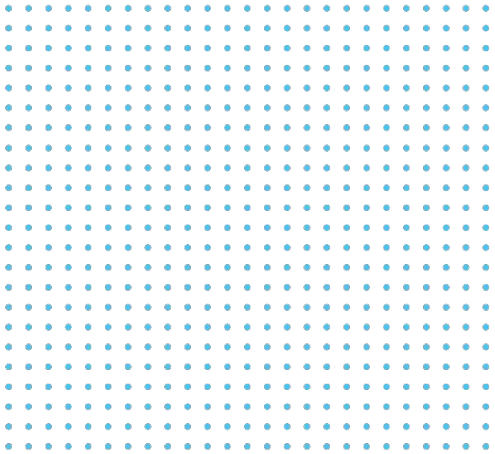
Lorna L. Waggoner
ecfirst - HIPAA Trainer
HIMSS Iowa Sponsorship
National HIMSS Chapter Task Force



Agenda

- Healthcare - we have a problem.
- We are not the only ones.
- There is a solution.
- Overview of frameworks.
- Next steps.



Billions are being spent of fines, penalties, class action lawsuits and false claims

HIPAA breaches can result in significant fines and penalties, particularly when they involve large-scale data breaches such as those that have affected major organizations.

Anthem Inc.: In 2018, Anthem paid $16 million to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) for HIPAA violations following a cyberattack that exposed the ePHI of nearly 79 million people.

Additional State-level settlements: In addition to the federal fine, Anthem also agreed to settle with 43 U.S. states and the District of Columbia for a combined $39.5 million. This state-level settlement was meant to resolve state attorneys general investigations into the breach.

Excellus Health Plan: In 2021, Excellus agreed to pay $5.1 million to settle potential HIPAA violations related to a data breach that affected over 9.3 million individuals.

Hmmm…..I wonder if this has anything to do with the cost of insurance premiums?

What is "Reasonable and Appropriate"

On June 5, 2021, H.R. Bill 7898

HIPAA Safe Harbor Law was passed and signed by then President Trump.

This bill addresses health information technology provisions concerning cybersecurity practices and information blocking.

The Department of Health and Human Services (HHS) may reduce fines and penalties for violations of certain federal privacy and security standards for health information if an entity subject to those standards has adopted specific cybersecurity best practices.

The news release specifically mentions HITRUST CSF and the NIST cybersecurity framework.

This announcement in 2021 now clearly states what "Reasonable and Appropriate" means for HIPAA compliance!

Burying your head in the sand will not cover your tail!

Headline 11/4/2024

Doctor Hit With $500K HIPAA Fine: Feds Worse Than Hacker

Plastic Surgeon Paid $53K Ransom But Says 'the Real Criminal' Is HHS.

- South Dakota plastic surgery clinic, recalled the day in 2017, a hacker locked up nine workstations and two servers with ransomware. (Have they done a Risk Analysis, policies in place, was it internal or external)
- He ended up paying $53,000 in ransom to access the data, and he claims no data was stolen. (Was it copied or altered is it correct)
- Nearly, seven years later after paying a $500,000 HIPAA fine, doctor alleges he got better treatment from the cybercriminals than he did federal regulators. (The fine would not have been that high if he had followed the Safe Harbor Law of 2021)
- In the article the provider commented that the government is to protect him from having these issues. They wrote the guidelines; he has to do the work!

Since 2018, the number of in large breaches involving ransomware attacks reported to HHS OCR has grown 264%.

Other Industries Regulatory fines

PCI DSS (Payment Card Industry Data Security Standard)

Target: In 2017, Target agreed to pay $18.5 million as part of a settlement with 47 states and the District of Columbia following a data breach that compromised 40 million credit and debit card accounts.

Home Depot: In 2017, Home Depot agreed to a $25 million settlement related to a data breach that affected 56 million credit card numbers.

GDPR (General Data Protection Regulation)

Meta (Facebook): In 2023, Meta was fined €1.2 billion by the Irish Data Protection Commission for GDPR violations related to data transfers.

Amazon: In 2021, Amazon received a €746 million fine from Luxembourg's data protection authority for GDPR violations related to processing personal data.

Are the cost of goods going up from inflation or lack of proactive cybersecurity program?

Whistle Blowers and False Claims Act

Whistleblower Laws

Deutsche Bank: In 2021, Deutsche Bank agreed to pay $130 million to resolve allegations that it violated the Foreign Corrupt Practices Act (FCPA) by concealing bribes paid to foreign officials. Part of the settlement was influenced by whistleblower reports.

Cisco Systems: In 2019, Cisco agreed to pay $8.6 million to settle a whistleblower lawsuit alleging that the company sold video surveillance software with known security vulnerabilities.

FCA (False Claims Act)

Reckitt Benckiser Group: In 2019, Reckitt agreed to pay $1.4 billion to resolve allegations under the False Claims Act related to the marketing of the opioid addiction treatment drug Suboxone.

Novartis: In 2020, Novartis agreed to a $642 million settlement for paying kickbacks to doctors to induce them to prescribe their medications.

Whistle Blowers get 15% - 30% of the settlements plus cost for lawyer fees!

Other Notable Fines

Uber: In 2018, Uber was fined $148 million in a settlement with U.S. states over a data breach cover-up.

British Airways: In 2020, British Airways was fined £20 million by the UK for a data breach.

Have your vacation or business travel costs gone up lately?

We need you to take a seat at the table, maybe not as expert but as a participant. Dig in, speak up, and make it happen!

This is everyone's problem now, not just IT.

Key Cybersecurity Laws and How They Can Impact Your Business

Key points to remember:

- These regulations are the same, only different!
- Often don't change over time always have Access Control.
- How you control access changes as the world changes.
- Hard for everyone to know everything.

- **Year:** Represents the year the regulation/framework was effectively implemented or significantly updated.
- **Full Name:** Most of these are known by the acronym this is regulations full name.
- **Scope:** Describes the general area or industry to which the regulation/framework applies.
- **Objective:** Summarizes the main goal or purpose of the regulation/framework.
- **Focus:** Indicates the primary areas of focus within the regulation/framework.
- **Enforcement:** Identifies the entities responsible for enforcement and compliance monitoring.

Regulation	Year	Name	Scope	Objective	Focus	Enforcement
HIPAA	1996	Health Insurance Portability and Accountability Act	Healthcare providers, plans, and clearinghouses	Protect patient health information	Privacy and security of health information	U.S. Department of Health and Human Services (HHS) and Office for Civil Rights (OCR)
COBIT	1996	Control Objectives for Information and Related Technologies	IT governance and management framework	Optimize IT governance and management	IT processes and controls	Information Systems Audit and Control Association (ISACA)
FISMA	2002	Federal Information Security Management Act	Federal agencies	Protect government information and operations	Information security	Office of Management and Budget (OMB)
PCI DSS	2004	Payment Card Industry Data Security Standard	Organizations handling cardholder data	Protect cardholder data	Payment card security	PCI Security Standards Council
ISO 27000 Series	2005	International Organization for Standardization	Organizations of all types	Provide a framework for information security management	Information security management systems	International Organization for Standardization (ISO)
HITRUST CSF	2007	Health Information Trust Alliance (now HITRUST)	Healthcare and other industries	Provide a comprehensive framework for managing information risk	Information security and risk management	HITRUST Alliance
Zero Trust	2010's	Zero Trust	Federal agencies and organizations	Implement a zero trust architecture	Continuous verification of user and device identity	Office of Management and Budget (OMB)
SOC 2	2010	System and Organization Controls 2	Service organizations	Ensure service providers securely manage data	Security, availability, processing integrity, confidentiality, privacy	American Institute of Certified Public Accountants (AICPA)
FedRAMP	2011	Federal Risk and Authorization Management Program	Cloud service providers to federal agencies	Standardized security assessment for cloud products and services	Cloud security	General Services Administration (GSA)
NIST SP 800-171	2015	National Institute of Standards and Technology, NIST (Special Publication 800-171	Non-federal systems handling Controlled Unclassified Information (CUI)	Protect the confidentiality of CUI	Information security	National Institute of Standards and Technology (NIST)
GDPR	2018	General Data Protection Regulation	Organizations processing EU residents' personal data	Protect personal data and privacy	Data protection and privacy	European Data Protection Board (EDPB)
CMMC Level 1 and 2	2024	Cybersecurity Maturity Model Certification	Defense contractors	Ensure cybersecurity practices in	Cybersecurity maturity	U.S. Department of Defense (DoD)

There are others too

Trusted Exchange Framework and Common Agreement (TEFCA) launched by the U.S. Department of Health and Human Services (HHS) to promote a nationwide health information exchange.

Sarbanes Oxley (SOX) is to protect investors by improving the accuracy and reliability of corporate financial disclosures.

Canada has the Personal Information Protection and Electronic Documents Act (PIPEDA).

India has Digital Personal Data Protection Act 2023 (DPDP Act).

Next Steps

- *Read about the issues in all industries.*
- *Attend conferences (HIMSS, AHA, ISACA).*
- *Ask questions.*
- *Offer your input.*
- *Don't let things slide.*
- *Everything matters!*

Q & A