

The 28th National HIPAA Summit

NIST CsF = Standard for HIPAA Compliance + Cybersecurity



Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)
CCSFP (HITRUST), Member (FBI) InfraGard



Agenda

The 28th National
HIPAA Summit



The 28th National HIPAA Summit

Infographic

HIPAA & HITECH: Fast Facts

Meaningful Use & MIPS Measures Mandate HIPAA Security

- Meaningful Use (MU) and MIPS Measures requires organizations to ensure a comprehensive and thorough security risk assessment is performed.
- Ensure technical vulnerability assessment and pen tests of mission critical applications and assets.

Risk Assessment & Management

Risk Assessment
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

Risk Management
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.



World-Class Signature HIPAA Methodology



HITECH Breach

- Breaches must be reported to OCR
- A breach is treated as discovered on first day the breach is known to the covered entity or business associate.

HIPAA Privacy Rule

- Establishes federal standards to safeguard the privacy of personal health information.
- Gives patients an array of rights with respect to their medical information.
- Provides the foundation for the HIPAA Security Rule.

HIPAA Security Rule

- Emphasizes confidentiality, integrity, and availability of all electronic Protected Health Information (ePHI).
- Establishes national standards to protect individuals' ePHI that is created, received, used, or maintained by an organization.
- Requires appropriate safeguards to ensure the confidentiality, integrity, and security of ePHI.
 - Administrative Safeguards
 - Physical Safeguards
 - Technical Safeguards
 - Policies & Procedures and Documentation Requirements
 - Organizational Requirements



2019

Handwritten signature: Hedy Ali Pasha



Active Cyber Defense!

State of Cybersecurity Mandates

- NY 500 CRR**
- New York State Cybersecurity Requirements for Financial Services Companies
 - A standards-based framework to improve protection of client's personal information
 - Affects healthcare organizations also, such as health insurers, and their business associates
 - Full compliance required by March 2019 when transition period ends
 - Future of cybersecurity regulations likely to see from other U.S. states
- New York

- HB 300**
- Increases civil/criminal penalties for wrongful disclosure of PHI
 - Revises definition of a covered entity
 - Requires customized staff training
 - Stricter than HIPAA
- Texas



- GDPR**
- Covers every industry, and every individual in the European Union (EU)
 - Applies to companies outside EU who offer goods and services to or monitor behavior of EU data subjects
 - It is about data flows with which data is accessed and abused
 - Effective May 25, 2018
- European Union

HITRUST CSF

1 Information Protection Program	11 Access Control
2 Endpoint Protection	12 Audit Logging & Monitoring
3 Portable Media Security	13 Education, Training & Awareness
4 Mobile Device Security	14 Third Party Assurance
5 Wireless Security	15 Incident Management
6 Configuration Management	16 Business Continuity & Disaster Recovery
7 Vulnerability Management	17 Risk Management
8 Network Protection	18 Physical & Environmental Security
9 Transmission Protection	19 Data Protection & Privacy
10 Password Management	

- ISO 27001**
- A global standard for information security
 - Includes dozens of standards in the 27000 family
 - Provides a systematic approach to secure sensitive information
 - Applicable to all industries, and businesses of all sizes
- Global

- California**
- SB 1386
 - SB 541
 - AB 1750
 - SB 24
 - AB 1278
 - AB 1710
 - AB 211



- 201 CMR 17.00**
- Impacted entities must develop a written information security program
 - Up-to-date firewall, operating system and malware protection
 - Review of security measures at least annually
- Massachusetts

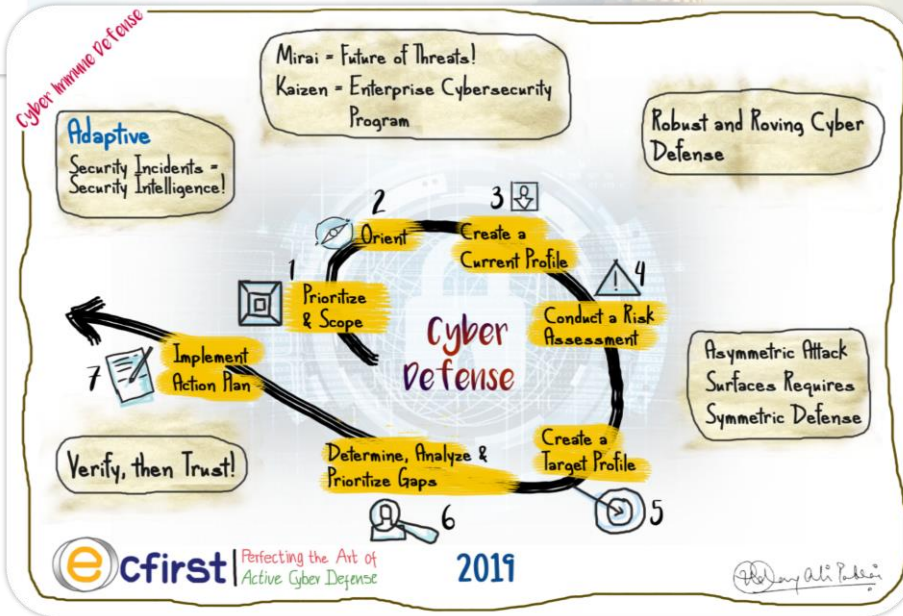


2019

Handwritten signature: Hedy Ali Pasha



The 28th National HIPAA Summit



eCfirst HITRUST Authorized CSF Assessor

The 28th National HIPAA Summit

2020 Mandates

eCfirst HITRUST Authorized CSF Assessor

SB 327 Information Privacy: Connected Devices

The 28th National HIPAA Summit

Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

- ∞ Effective **January 1, 2020**
- ∞ SB 327 requires manufacturers of connected devices to equip the device with reasonable security features that are appropriate to the nature and function of the device, appropriate to the information it may *collect, contain, or transmit*
- ∞ Designed to protect the device and any information contained therein from *unauthorized access, destruction, use, modification, or disclosure*



GDPR: European Standard CCPA: California Impact

The 28th National HIPAA Summit



California Consumer Privacy Act (CCPA)

The 28th National HIPAA Summit

CCPA grants California residents the right:

Effective **January 1, 2020**



To know what personal information is being collected about them.



To know whether their personal information is sold or otherwise disclosed and to whom.



To say no to the sale of their personal information.



To access their personal information and request deletion under certain circumstances.



To receive equal service and price, even if they exercise their privacy rights.

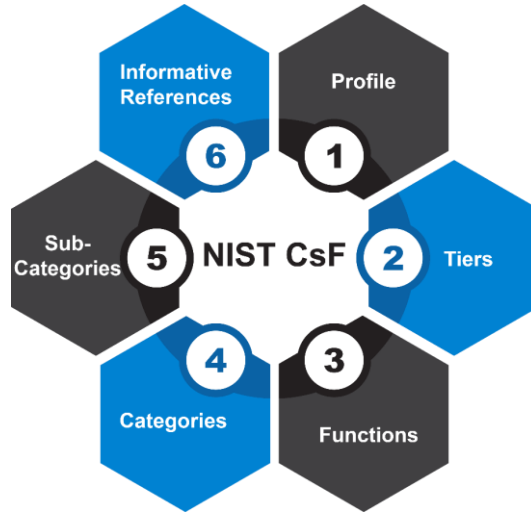


The 28th National HIPAA Summit



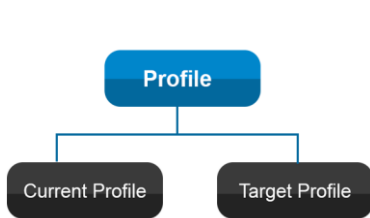
NIST CsF

The 28th National HIPAA Summit

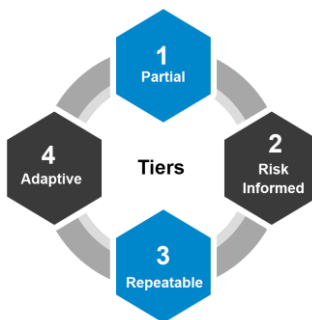


NIST CsF: Organization

The 28th National HIPAA Summit



Profile



Tiers



Functions



Function and Category Unique Identifiers

The 28th National HIPAA Summit

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
ID	Protect	PR.AC	Identify Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
RS	Respond	RS.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.JM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



Enterprise Risk Assessment

The 28th National HIPAA Summit



- 1 Conduct a VA
- 2 Validate & Remediate Findings
- 3 Pen Test



NIST CSF/HIPAA Mapping

The 28th National HIPAA Summit

#	NIST CsF v1.1 Controls Mapping	HIPAA Security Rule Standards & Implementation Specifications
Identify (ID)		
1	ID.AM-1: Physical devices and systems within the organization are inventoried.	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC
		164.310(a)(2)(ii) Facility Security Plan (A) SPEC
		164.310(d)(1) Device and Media Controls SPEC
2	ID.AM-2: Software platforms and applications within the organization are inventoried.	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC
		164.308(a)(7)(i)(E) Applications and Data Criticality Analysis (A) SPEC
3	ID.AM-3: Organizational communication and data flows are mapped.	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC
		164.308(a)(3)(ii)(A) Authorization and/or Supervision (A) SPEC
		164.310(d)(1) Device and Media Controls SPEC
4	ID.AM-4: External information systems are catalogued.	164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Function (R) SPEC
		164.308(b)(1) Business Associate Contracts and Other Arrangements SPEC
		164.314(a)(1) Business Associate Contracts or Other Arrangements STD
		164.314(a)(2)(i) Business associate contracts SPEC
		164.314(a)(2)(ii) Other arrangements SPEC
		164.316(b)(2)(i) Time Limit (R) SPEC



HIPAA Cybersecurity Program

The 28th National HIPAA Summit

NIST CsF

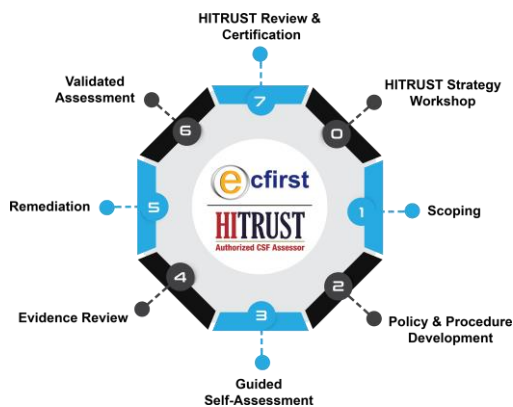




Next Steps



HITRUST + NIST Certification



HITRUST / NIST Certification Roadmap



Establish a Credible HIPAA Program!



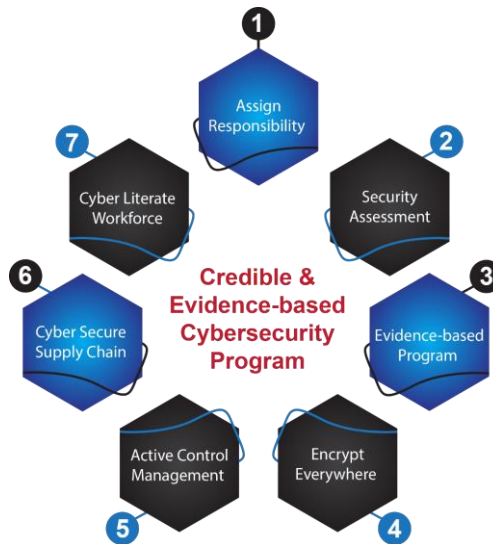
HIPAA Cybersecurity Program: *Five Dimensions Aligned*

The 28th National HIPAA Summit



Cyber Immune Defense

The 28th National HIPAA Summit



Cyber Action Required Annually!

The 28th National HIPAA Summit

- 1 Develop a credible cybersecurity strategy
- 2 Conduct a comprehensive security risk assessment
- 3 Ensure a technical vulnerability assessment is performed quarterly, and a pen test annually
- 4 Perform a Business Impact Analysis (BIA)
- 5 Develop a detailed Disaster Recovery Plan (DRP)
- 6 Create a cyber incident response plan
- 7 Implement a cybersecurity framework (e.g. HITRUST, NIST CSF)



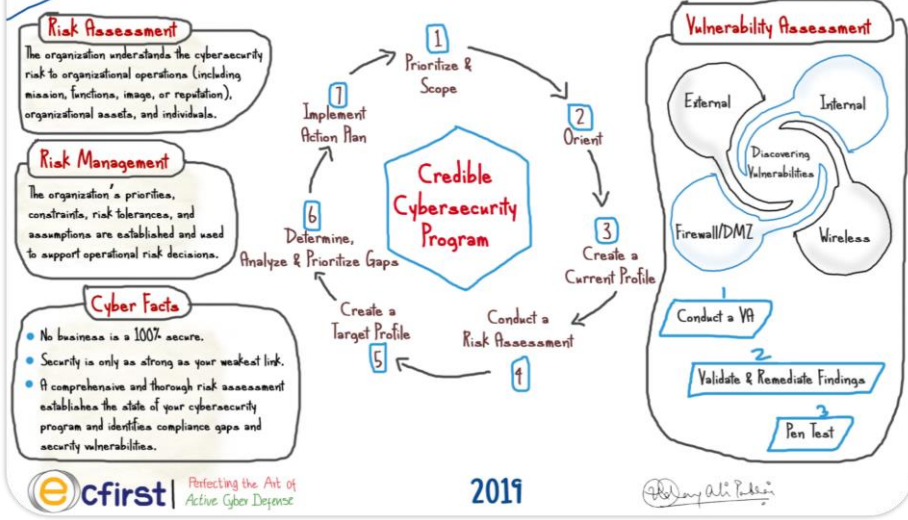
Lifecycle approach



Active Cyber Defense!

Cyber Risk Assessment & Management

The 28th National HIPAA Summit



A Cyber Brief

2020 Cybersecurity Mandates

The 28th National HIPAA Summit

CCPA Key Facts

- Is effective January 1, 2020
- Private right of action for California residents
- Grants new enforcement power to the Attorney General with high damages recoverable

CCPA Individual Rights

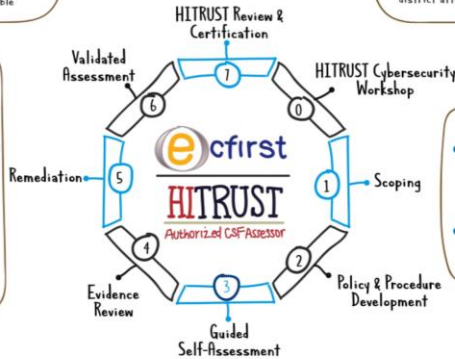
- What personal information is being collected about them
- Whether their personal information is sold or otherwise disclosed and to whom
- To say no to the sale of their personal information
- To access their personal information and request deletion under certain circumstances
- To receive equal service and price

California

- SB 1386
- AB 1450
- AB 1298
- AB 211
- SB 541
- SB 24
- AB 1710

SB 327 Key Facts

- Is effective January 1, 2020
- Focused on security features of IoT devices to protect personal information
- California attorney general, county counsel and district attorneys will enforce the bill



SB 327 Key Actions Required

- Businesses should familiarize themselves with industry standards and applicable guidance relating to IoT device security
- Businesses subject to compliance should now to build "security by design" into the manufacturing processes

ecfirst | Perfecting the Art of Active Cyber Defense

2019

Handwritten signature: Mary Ali Parker

ecfirst | HITRUST Authorized CSF Assessor

U.S. Government Cyber Standard

NIST Cybersecurity Framework (CsF)

The 28th National HIPAA Summit

Framework Functions

Function	Categories	Subcategories	Informative References
IDENTIFY	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
PROTECT	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
DETECT	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
RESPOND	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
RECOVER	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

Functions

Function	Category
Identify	Risk Management
	Business Environment Governance
	Risk Assessment
	Risk Management Strategy
Protect	Supply Chain Risk Management
	Identify Management and Access Control
	Awareness and Training
	Data Security
Detect	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Respond	Incident Response and Recovery
	Security Continuous Monitoring
Recover	Defection Processes
	Response Planning
Communications	Analysis
	Mitigation Improvements
Recovery Planning	Improvements
	Communications



ecfirst | Perfecting the Art of Active Cyber Defense

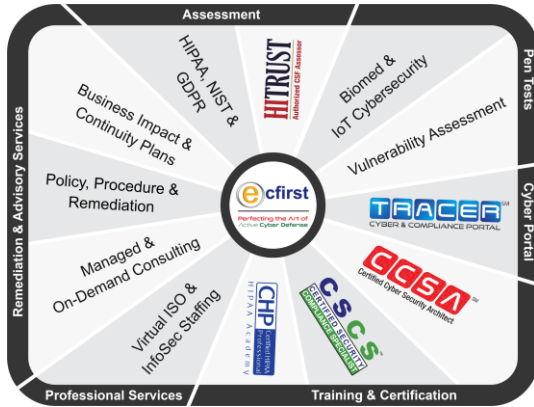
2019

Handwritten signature: Mary Ali Parker

ecfirst | HITRUST Authorized CSF Assessor

About ecfirst

The 28th National HIPAA Summit



VISION (Mantra)

Enabling establishment of an active cyber defense program and capability.



MISSION (Karma)

Implement an evidence-based compliance program integrated within an enterprise-wide active cyber defense system.



OUR PROMISE

- Unconditional Guarantee. No Questions!
- ecfirst will not consider an engagement complete unless client is 100% satisfied.

Delivering Everything Compliance. Everything Security.
1000s of Clients | Clients in all 50 States | Clients on 5 Continents



Certification Training

The 28th National HIPAA Summit



Certified HIPAA Professional



Certified Security Compliance Specialist™



Certified Cyber Security ArchitectSM



HITRUST Cybersecurity Strategy Workshop



Thank You!

The 28th National
HIPAA Summit



+1.949.528.5224

Ali.Pabrai@ecfirst.com



ecfirst

HITRUST
Authorized CSF Assessor