

Nov 4, 2019

Health Care Compliance Association | **HCCA**

Privacy and Compliance, HIPAA State Law and GDPR

Iliana Peters, Shareholder, Polsinelli, PC
Ali Pabrai, Global Cybersecurity & Compliance Expert
CEO, ecfirst

GDPR **HIPAA**
Privacy
NIST Cybersecurity Framework
NIST IR 8228 **CCPA**
Threats

ecfirst

1

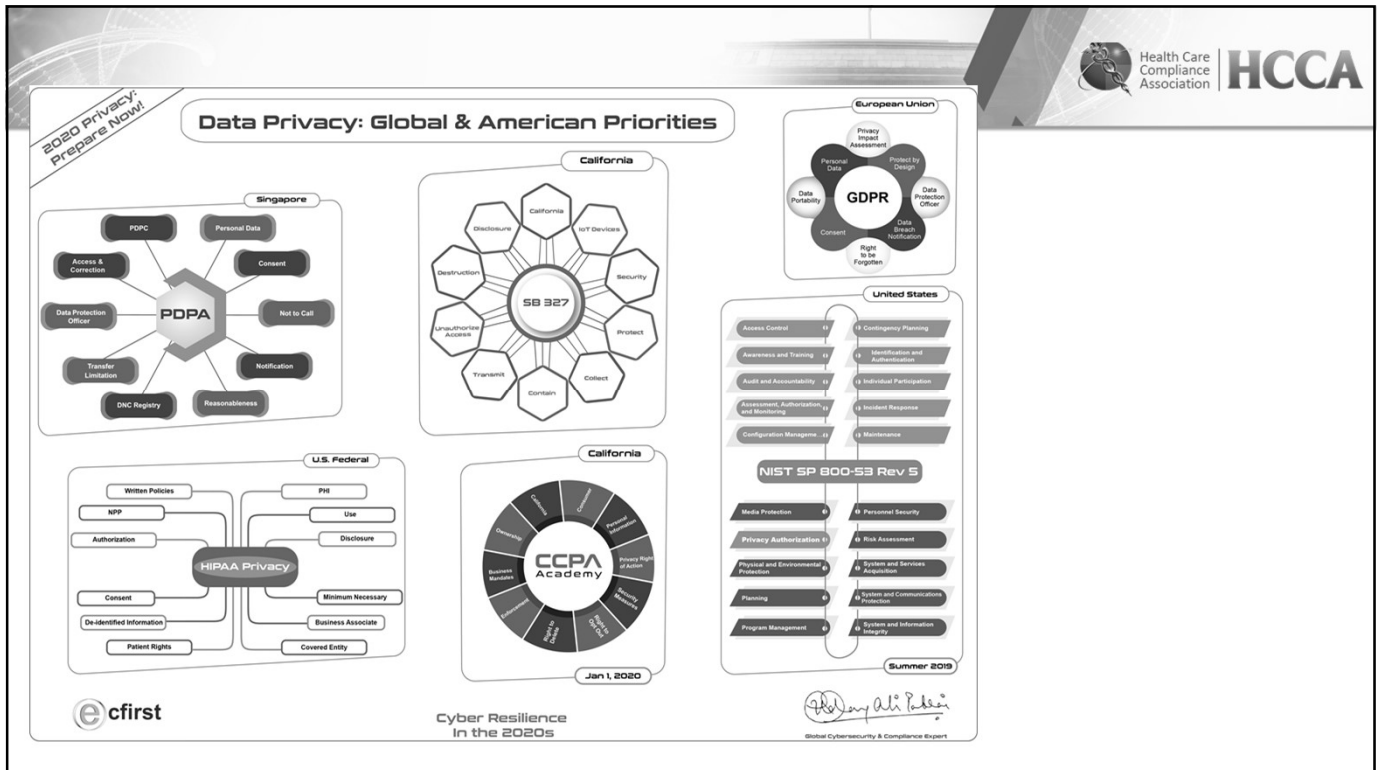
Agenda

Health Care Compliance Association | **HCCA**

- Privacy: Global State
- HIPAA Settlements
- General Data Protection Regulations (GDPR)
- California Consumer Privacy Act (CCPA)
- NIST Cybersecurity Framework

1

2



3

Health Care Compliance Association | HCCA

\$ LAW

HIPAA Settlements

OCR and State Attorney Generals

4

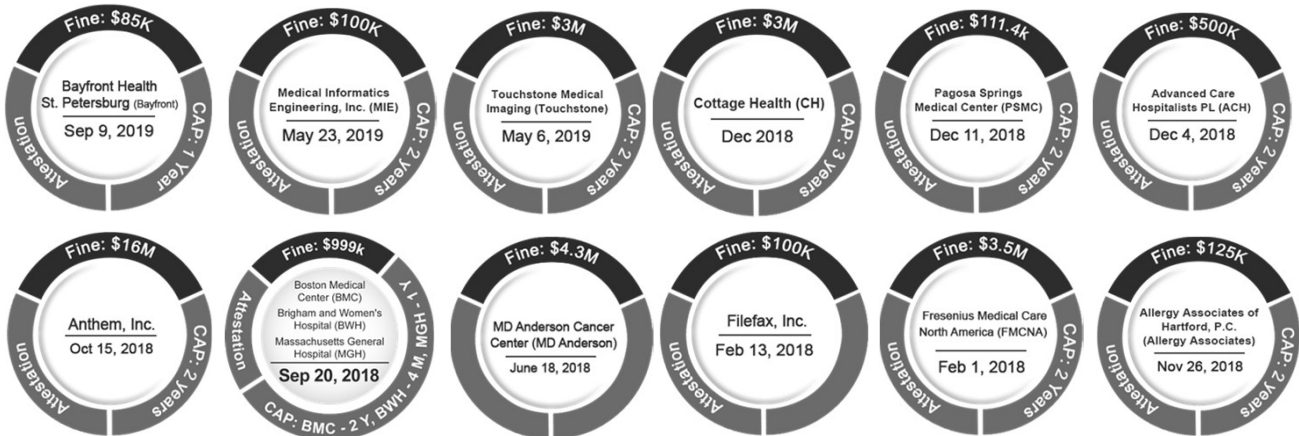
State of HIPAA Compliance



Health Care
Compliance
Association

HCCA

Total Settlements: \$31,820,400



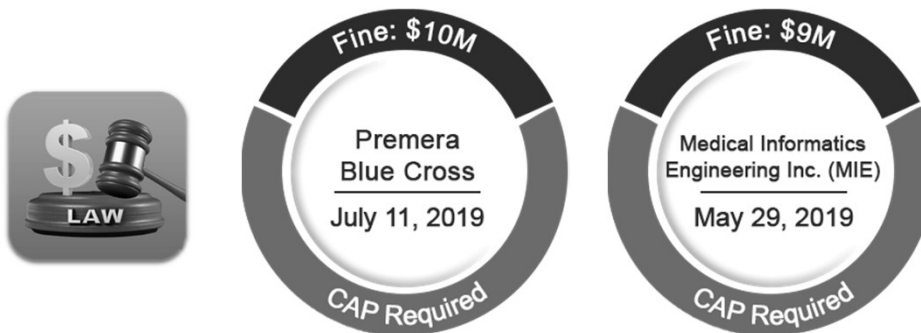
5

Summary! 2019 HIPAA Fines by State Attorney Generals



Health Care
Compliance
Association

HCCA



6

HIPAA Settlements by State Attorney Generals Premera Blue Cross



- Premera Blue Cross, paid \$10 million to 30 states following an investigation into a data breach that exposed personal information on more than 10 million people across the country.
- Premera will spend \$74 million to settle a federal class-action lawsuit on behalf of affected customers.
- In addition to the monetary penalty, Premera is required to ensure its data security program is adequate to protect health data as required by law.
- From May 5, 2014 until March 6, 2015, a hacker had unauthorized access to the Premera network containing ePHI, including private health information, Social Security numbers, bank account information, names, addresses, phone numbers, dates of birth, member identification numbers and email addresses.
- The coalition of 30 state attorneys general, led by Washington State Attorney General Bob Ferguson, investigated Seattle-based Premera's cybersecurity vulnerabilities that gave a hacker unrestricted access to ePHI for nearly a year.

7

HIPAA Settlements by State Attorney Generals Medical Informatics Engineering (MIE)



- MIE reached a \$900,000 settlement in the country's first federal multistate lawsuit, over a 2015 data breach that impacted 3.5 million patients.
- Between May 7 and May 26, 2015, hackers gained access to a server containing data related to its NMC service. Names, addresses, usernames, passwords, and ePHI were potentially accessed and stolen.
- Hackers infiltrated a MIE Web application and accessed its records on more than 3.9 million individuals. The data included sensitive medical and financial information such as Social Security numbers, lab results, medical conditions and health plan records.
- Eleven of MIE's clients and 44 radiation centers were affected, along with nearly 200 provider clients of MIE subsidiary NoMoreClipboard (NMC), which markets personal health records to health care providers, to employers and directly to consumers.
- Indiana-based MIE undertook to notify all affected individuals, but some employer and health care provider clients reached out to their employees and patients as well, in part to minimize confusion.
- MIE was sued by 16 states following a 2015 data breach.

8



General Data Protection Regulations (GDPR)

9

GDPR Fast Facts



10

GDPR Settlement: Marriott



- July 9, 2019, the Information Commissioner's Office (ICO) issued a notice of its intention to fine Marriott International £99,200,396 for violating the EU's GDPR.
- The hotel group, which suffered a breach last year, could face a fine of over £99 million (\$123 million).
- The fine relates to an incident that Marriott brought to the ICO's attention in November 2018.
- A variety of personal data containing approximately 339 million guest records were exposed by the incident.
- Approximately 30 million records were thought to relate to residents of 31 countries in the European Economic Area (EEA), with 7 million related to UK residents.
- It is believed the vulnerability began with systems of the Starwood hotel group that were compromised in 2014. Marriott acquired Starwood in 2016, but the exposure was not discovered until 2018.
- The ICO found that Marriott failed to undertake sufficient due diligence when it bought Starwood.

11

GDPR Settlement: British Airways



- July 8, 2019, the ICO issued notice of its intent to fine British Airways £183.39 million for GDPR infringements.
- British Airways notified the ICO of the incident in September 2018 after suffering a cyberattack in September last year.
- Hacker had stolen payment card data associated with 380,000 transactions including bank card numbers, expiry dates and cvv codes.
- transactions details were taken via malicious script designed to steal financial information by skimming BA's payment page before it was submitted.
- The attack, thought to be perpetrated by the same group that hit Ticketmaster, Magecart, would allow adversaries to see people's details as they were entered on the page.
- The ICO found that the company had poor security arrangements which compromised a variety of data, including log in, payment card, and travel booking details as well name and address information.

12



California Consumer Privacy Act (CCPA)

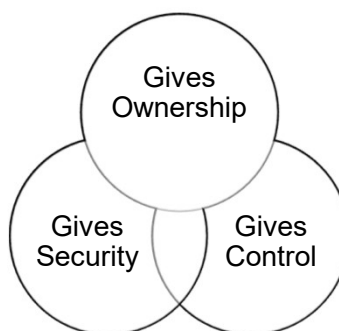
13

CCPA Fast Facts



Key Facts

- Effective January 1, 2020.
- Enforced July 1, 2020.
- Privacy rights for California residents.
- Grants new enforcement power to the Attorney General.



14

CCPA Individual Rights



What personal information is being collected about them.



Whether their personal information is sold or otherwise disclosed and to whom.



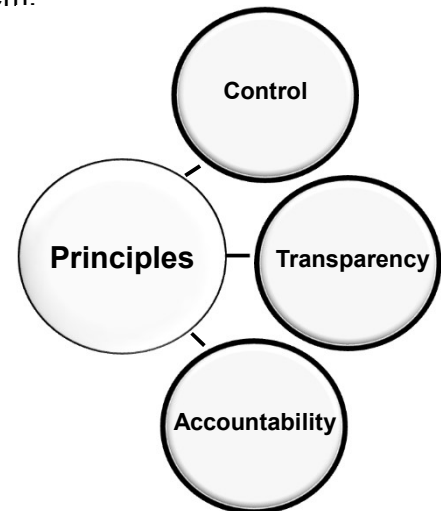
To say no to the sale of their personal information.



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



To receive equal service and price.



15

CCPA Consumer Rights, A Summary



Right to Knowledge	Right to be Forgotten	Right to Control Who has Access to their Information
<p>Consumers have the right to request information about:</p> <ul style="list-style-type: none"> What information a company is collecting about them How that information will be used If and with whom that information will be shared 	<ul style="list-style-type: none"> Companies must delete all information they have about a consumer at the consumer's request. Exceptions include: <ul style="list-style-type: none"> Data being processed and retained to complete a consumer-requested transaction Specific research purposes Limited analytical used Other regulatory and contractual exceptions 	<ul style="list-style-type: none"> Consumers must be able to opt out of the sale of their information to third parties.

16

CCPA Enforcement and Penalties



CCPA Penalties		
For non-compliance	Unintentional	\$2,500
	Intentional	\$7,500
If personal information is exposed in a data breach	Per incident	\$100–\$750 or greater if the actual damages exceed \$750

17

CCPA: 7 Key Steps



- 1 Establish Responsibility
- 2 Perform a comprehensive and thorough risk assessment, inclusive of a technical cybersecurity assessment
- 3 Update policies and procedures to address CCPA
- 4 Remediate gaps for CCPA compliance as identified in the risk assessment
- 5 Review cybersecurity supply chain (e.g. business associates), including update to contracts/agreements to determine appropriate protection for all California resident data
- 6 Train members of the workforce to raise higher awareness of CCPA requirements
- 7 Monitor capabilities implemented actively to ensure appropriate management of controls

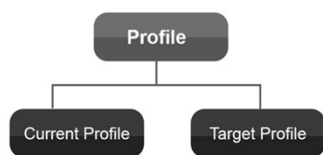
18



NIST Cybersecurity Framework

19

NIST Cybersecurity Framework



20

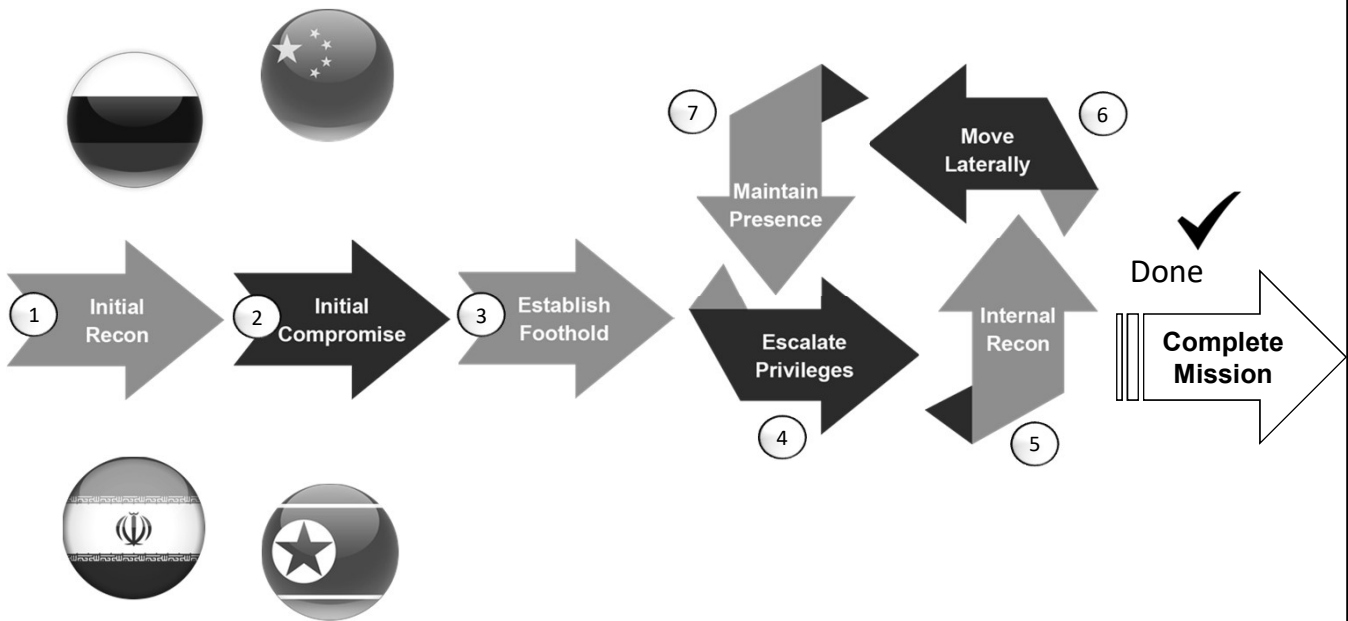
NIST Cybersecurity Framework: Foundation for Cybersecurity



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
PR	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
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

21


Cyber-attacks: Global & Sophisticated



22

U.S. Government Cyber Standard

NIST Cybersecurity Framework



Framework Functions


Function	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			


Functions

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
	Identify Management and Access Control
Protect	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology


Functions

Function	Category
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
Recover	Mitigation Improvements
	Recovery Planning
	Improvements






Cyber Resilience In the 2020s




Global Cybersecurity & Compliance Expert





23


U.S. Government Cyber Standard



Perfecting the Art of Active Cyber Defense







24



Health Care Compliance Association | **HCCA**

Thank You!

 **Iliana Peters**

Ali Pabrai | Ali.Pabrai@ecfirst.com | +1.949.528.5224



25