

Federal and State Privacy Laws: Practical Issues and Implications

Suffolk Univ. Law School
Professor Landers

October 4, 2023

COLIN J. ZICK
Co-Chair, Privacy and Data
Security Practice
FOLEY HOAG LLP
czick@foleyhoag.com
617 832-1275



Colin J. Zick

Partner and Co-Chair, Health Care and Privacy & Data Security Practice Groups
Boston | +1.617.832.1275 | czick@foleyhoag.com



- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.
- Advises on issues involving the transfer of data between jurisdictions, including GDPR, EU-US Privacy Shield, CCPA, CPRA, and other data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.
- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com. Serves as a member of Law360's Privacy & Consumer Protection editorial advisory board.
- Selected by his peers for inclusion in THE BEST LAWYERS IN AMERICA in the fields of Healthcare Law (2015-present) and Privacy and Data Security (2018-present)
- Ranked by CHAMBERS USA: AMERICA'S LEADING LAWYERS FOR BUSINESS as one of Massachusetts' leading Healthcare attorneys (2010-present)

Practicing privacy and data security law: what does it mean?

- Help clients understand and maneuver through issues and manage risks related to their sensitive data
- Provide advice that address the myriad legal and policy challenges:
 - Complying with state, federal and international laws that govern privacy, information security, identity theft, and surveillance
 - Complying with HIPAA's privacy and security requirements
 - Assisting with state and federal investigations
 - Developing privacy and information security policies
 - Negotiating third-party data security agreements
 - Investigating, litigating and resolving security incidents, including competitive espionage and proprietary data leaks
 - Counseling on corporate governance
 - Advising clients on safeguarding company records, financial information and other valuable information assets

Understanding state, federal
and international laws, regulations
and agencies, including:

- ✓ Health Insurance Portability and Accountability Act (**HIPAA**)
- ✓ FTC Act
- ✓ General Data Protection Regulation (**GDPR**)
- ✓ California Consumer Privacy Act (**CCPA**)
- ✓ Computer Fraud & Abuse Act (**CFAA**)
- ✓ Electronic Communications Privacy Act, as amended by the U.S. PATRIOT Act
- ✓ Gramm-Leach-Bliley Act (**GLBA**)
- ✓ Children's Online Privacy Protection Act (**COPPA**)
- ✓ Family Educational Rights and Privacy Act (**FERPA**)
- ✓ Agencies including:



Ransomware is big, getting bigger

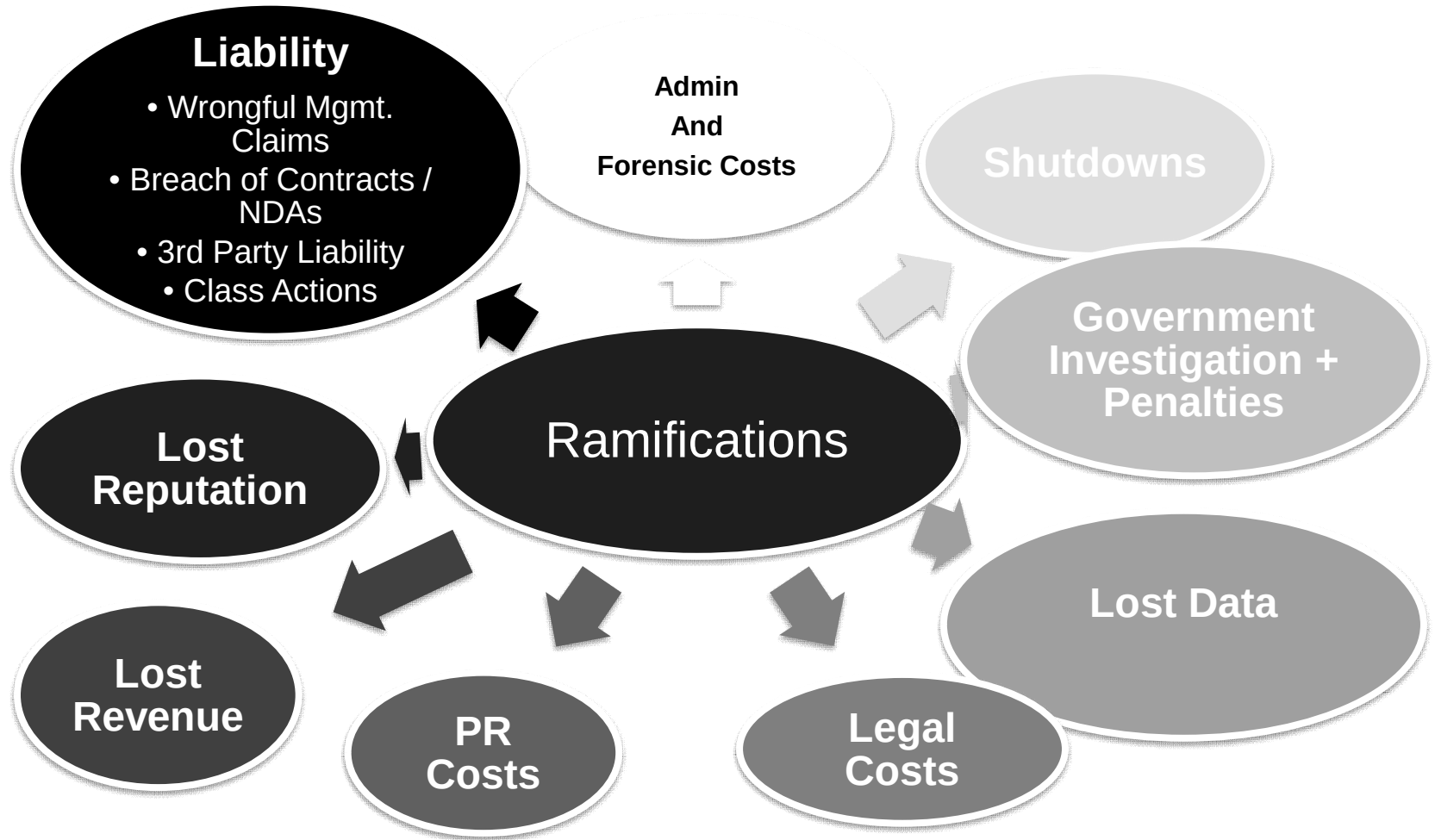
- From January to July 31, 2021, the IC3 received 2,084 ransomware complaints with over \$16.8M in losses, a 62 percent increase in reporting and 20 percent increase in reported losses compared to the same time frame in 2020. Source: cisa.gov
- During the first half of 2022, there were a total of **236.1 million** ransomware attacks worldwide. Overall, the number of ransomware attacks decreased rapidly between the second and fourth quarters of 2021, going from nearly 189 million cases to 133 million. Source: statistica.com
- Ransomware attacks resurged in early 2023:
 - new players such as Royal, BianLian, and Play ransomware gangs joined the field and major players like Lockbit and Clop executed mass-ransomware attacks.
 - The top targeted industries were manufacturing (19.5%), professional, scientific and technical services (15.3%) and educational services (6.1%). Source: <https://blackkite.com/whitepaper/ransomware-threat-landscape-2023/>

What is ransomware?

- This is a global intrusion campaign, affecting public and private organizations around the world.
- A formerly trusted event, business software updates, has been “trojanized” to distribute malware.
- Here are the 2023 HIPAA investigations regarding hacking in just Massachusetts:

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Nuance Communications, Inc.	MA	Business Associate	1225054	09/15/2023	Hacking/IT Incident	Network Server
	MedMinder Systems, Inc.	MA	Healthcare Provider	12146	09/01/2023	Hacking/IT Incident	Network Server
	Mountain View Family Practice, PC	MA	Healthcare Provider	5139	08/31/2023	Hacking/IT Incident	Electronic Medical Record, Network Server
	The University of Massachusetts Chan Medical School	MA	Business Associate	134394	08/21/2023	Hacking/IT Incident	Network Server
	Sovos Compliance LLC	MA	Business Associate	4563	08/08/2023	Hacking/IT Incident	Network Server
	Brigham and Women's Hospital	MA	Healthcare Provider	987	08/04/2023	Unauthorized Access/Disclosure	Other
	Tidewater Diagnostic Imaging, Ltd.	MA	Healthcare Provider	40195	06/26/2023	Hacking/IT Incident	Network Server
	Vitra Home Care, LLC	MA	Business Associate	658	06/22/2023	Hacking/IT Incident	Email
	New Horizons Medical, Inc.	MA	Healthcare Provider	12317	06/16/2023	Hacking/IT Incident	Network Server
	Elgon Information Systems	MA	Business Associate	31248	06/02/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	996	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	1389	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	1191	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	1518	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	524	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	507	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	983	05/26/2023	Hacking/IT Incident	Network Server
	Alvaria, Inc.	MA	Business Associate	803	05/26/2023	Hacking/IT Incident	Network Server

Ramifications of Privacy Incident



Close Encounters of the COVID Testing Kind

- “When is health information not *Protected Health Information*?”
- Does this distinction make any sense?
- What are the implications? For example, why do we treat differently your:
 - “Should I see my doctor” COVID test
 - “return to work” COVID test
 - “return to school” COVID test
 - “speak at the UN” COVID test
 - “I’m flying to Europe” COVID test
 - “I’m returning from Europe” COVID test
- Wearables/App data
 - Fertility/pregnancy
 - Pulse/Heart rate
 - Oxygen
- November 22, 2019:

“You Give Apps Sensitive Personal Information. Then They Tell Facebook.

Wall Street Journal testing reveals how the social-media giant collects a wide range of private data from developers; ‘This is a big mess’” <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>

The Lost World: FTC's health breach notification rule

- Show of hands: before today, who has heard of the FTC breach notification rule?
- 16 CFR Part 318: The Rule requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information. In addition, if a service provider to one of these entities has a breach, it must notify the entity, which in turn must notify consumers. The Final Rule also specifies the timing, method, and content of notification, and in the case of certain breaches involving 500 or more people, requires notice to the media.
<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule>
- Even the FTC seems to have forgotten about it, until recently.
<https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health>

FTC's Statement on Health App Breaches

STATEMENT OF THE COMMISSION
On Breaches by Health Apps and Other Connected Devices

September 15, 2021

In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 ("the Rule").¹

The FTC's Health Breach Notification Rule helps to ensure that entities who are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") nevertheless face accountability when consumers' sensitive health information is compromised. Under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations. The Rule also covers service providers to these entities. In practical terms, this means that entities covered by the Rule who have experienced breaches cannot conceal this fact from those who have entrusted them with sensitive health information.

The Rule was issued more than a decade ago, but the explosion in health apps and connected devices makes its requirements with respect to them more important than ever. The FTC has advised mobile health apps to examine their obligations under the Rule,² including through the use of an interactive tool.³ Yet the FTC has never enforced the Rule, and many appear to misunderstand its requirements. This Policy Statement serves to clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches.

The Rule covers vendors of personal health records that contain individually identifiable health information created or received by health care providers. The Rule is triggered when such entities experience a "breach of security."⁴ Under the definitions cross-referenced by the Rule, the developer of a health app or connected device is a "health care provider" because it "furnish[es] health care services or supplies."⁵ When a health app, for example, discloses

Zen and the Art of the HIPAA Business Associate Agreement

- Why are HIPAA business associate agreements ever negotiated?
- “I’m not a business associate, why do I still have to sign a business associate agreement?”
- I signed a business associate agreement – am I necessarily a business associate?
- What about those pesky subcontractors?
- Tricks of the trade
 - The contingent business associate agreement
 - Time for notice – *the Friday, December 24 breach*
 - Ownership, de-identification, and aggregation of data
 - Return or destroy data when the work is done?
- Add-ons:
 - State privacy laws
 - Indemnification
 - Limitation of liability
 - Insurance

Is a ransomware attack an “incident” or a “breach”?

- What’s the difference between an incident and a breach?
- Let’s look at the Sturdy Memorial example:

Notice of Data Security Incident

Sturdy Memorial Hospital (“Sturdy”) is committed to protecting the confidentiality and security of the information we maintain. We recently identified and addressed a data security incident that involved some patient information.

On February 9, 2021, we identified a security incident that disrupted the operations of our IT systems. We immediately took steps to secure our systems, launched a thorough investigation with the assistance of a third-party forensic investigator, and notified law enforcement. Through our investigation, we determined that an unauthorized party gained access to some of our systems during the morning of February 9, 2021. Our systems were secured later that same day. In exchange for a ransom payment, we obtained assurances that the information acquired would not be further distributed and that it had been destroyed.

On April 21, 2021, our review and analysis of the files involved in the incident determined that information belonging to Sturdy patients was contained in the files. The analysis also determined that information associated with patients of certain other healthcare providers - with which Sturdy previously partnered for the coordination of patient care – was also involved in the incident, including Harbor Medical Associates, South Shore Medical Center, and providers affiliated with South Shore Physician Hospital Organization.

The information involved may have included names, contact information – including address and phone number, dates of birth, Social Security numbers, Driver’s License numbers or other government issued identification numbers, financial account numbers, routing numbers and/or bank names, credit card numbers and security codes, Medicare Health Insurance Claim numbers, medical history information, treatment or diagnosis information, procedure or diagnosis codes, prescription information, provider names, medical record numbers, Medicare/Medicaid numbers, health insurance information, and / or treatment cost information. Note that our electronic health record system was **not** involved in the incident

Are There Civil Remedies?

“Judge prunes medical device company's lawsuit over exposed data”

- Customers claiming their PHI was exposed in the data breach filed a class action against Zoll in West Virginia state court in 2019. That case has been settled. Zoll sued its vendor who caused the breach.
- According to the complaint, Zoll, the manufacturer of the LifeVest wearable cardioverter defibrillator, hired Apptix Inc. in 2012 to securely store emails containing customer PHI. Apptix hired Sonian Inc. to provide software and services, and Sonian has since been acquired by Barracuda.
- In November 2018, a Barracuda employee inadvertently left a data port open, an error that went unremedied for seven weeks during which unauthorized third parties could access Zoll's emails. Barracuda notified Apptix of the data breach in January 2019, and Apptix notified Zoll, the complaint says.
- September 24, 2021 - A federal judge in Massachusetts has dismissed four of the five allegations Zoll Medical Corp. made against a cybersecurity company after a data breach exposed the protected health information of more than 277,000 patients. [Zoll Medical Corp. v. Barracuda Networks Inc. et al., No. 20-cv-11997, \(D. Mass. Sept. 22, 2021\).](#)
- Only a count alleging equitable indemnity will go forward; the judge dismissed the four other counts.

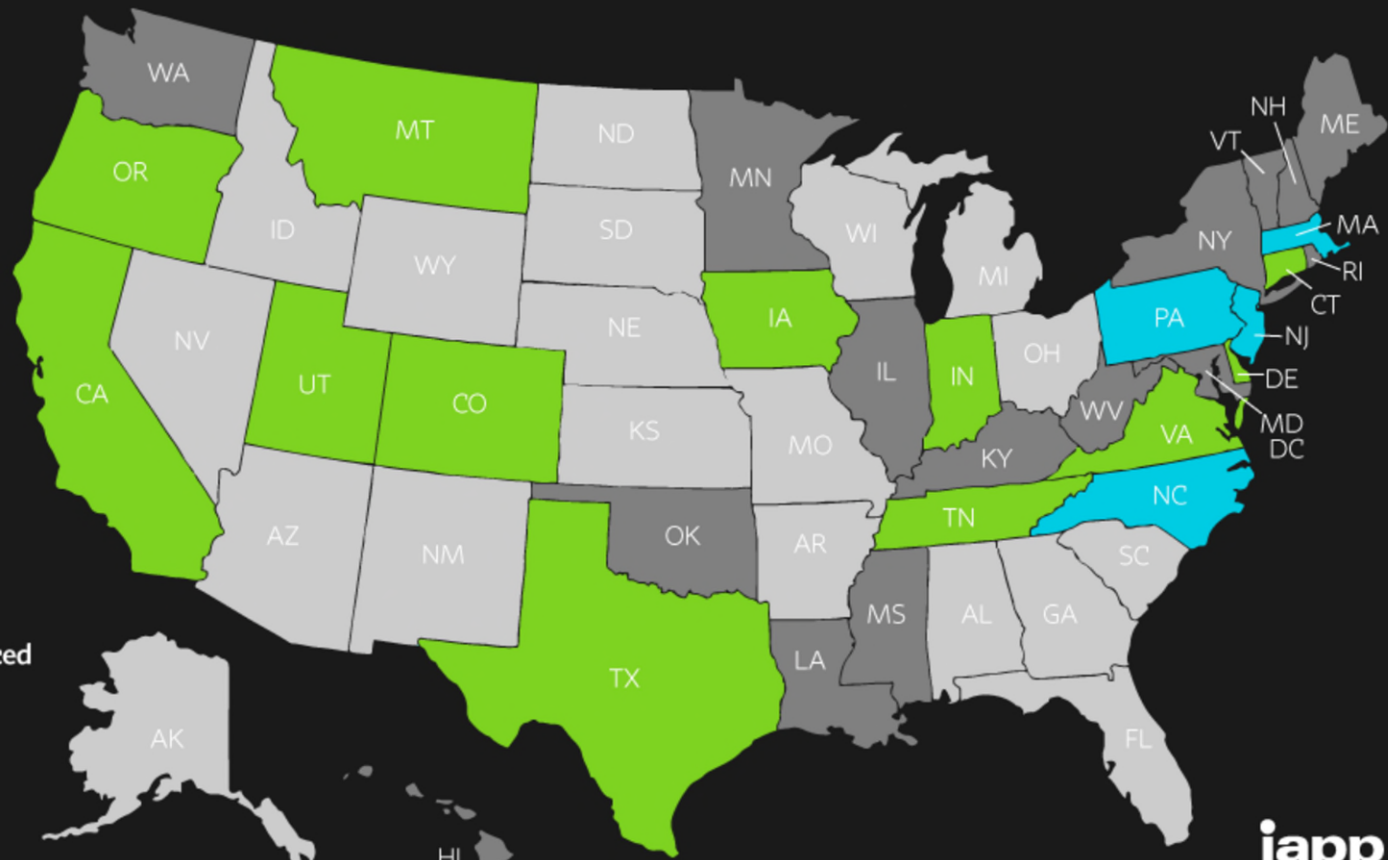
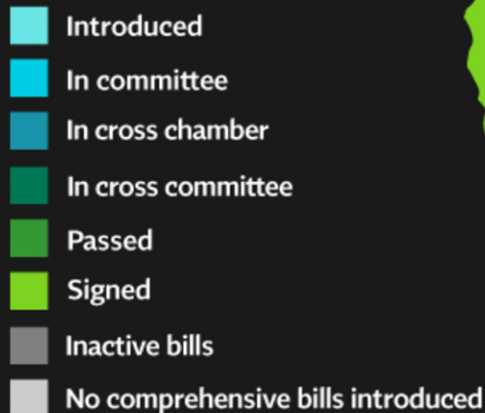
Source: Westlaw

State Privacy Laws Beyond California

- There are many privacy law developments in the 49 other states.

US State Privacy Legislation Tracker 2023

STATUTE/BILL IN LEGISLATIVE PROCESS



State-Level Regulation:

Data Privacy

- States passing comprehensive consumer privacy bills (influenced by EU data protection laws):
 - California
 - Colorado
 - Connecticut
 - Delaware
 - Indiana
 - Iowa
 - Montana
 - Oregon
 - Tennessee
 - Texas
 - Utah
 - Virginia
- In the absence of comprehensive federal regulation, states are filling the regulatory gaps.
- 4 other states with active bills
 - California
 - At the forefront
 - Several states have modeled their own statutes after the California CCPA and CPRA

Massachusetts: good ol' ch. 214, § 1B

- Chapter 214, § 1B: “A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.”
 - A violation constitutes an unfair or deceptive trade practice under the Commonwealth's consumer protection (Mass. Gen. Laws ch. 93A, § 1)
- Very sparse case law under this statute for years, but now activity is starting to ramp up, with increasing interest from the plaintiffs' bar.

A Recent ch. 214, § 1B Case

- Hartigan v. Macy's, Inc., (Civil Action No. 20-10551-PBS) (Nov. 5, 2020) (Saris, J.)
 - The plaintiff filed a complaint against Macy's following a cyberattack on Macy's customer database.
- Though plaintiff Robert Hartigan did not allege that the hackers misused his information after stealing it, he claimed the data breach nonetheless caused him emotional distress. He also claimed he suffered lost time and money remediating the situation by canceling his credit card, contacting each vendor that had his card number on file, and purchasing data-monitoring services to protect against future breaches.
- The defendant, Macy's, Inc., argued that such harms were insufficient to constitute an "injury-in-fact" that would confer standing to bring his claim.
- The court ruled that this Macy's customer whose name, address and credit card information were stolen in a cyberattack on the department store's online database lacked standing to bring a class action against the company under the Massachusetts privacy statute.
 - plaintiff had not alleged sufficient facts to support a substantial risk of future harm; and
 - his purchase of credit monitoring services was not "premised on a reasonably impending threat" and does not constitute injury-in-fact.

New York Rules & Regulations

- New York Stop Hacks and Improve Electronic Data Security (“SHIELD”) Act
 - Strengthens New York’s breach notification law by:
 - Broadening the circumstances for when a breach needs to be reported.
 - Requiring any persons who own or license NY residents’ personal data to implement a “data security program” providing “reasonable safeguards” to protect that data.
 - Gives AG enforcement authority; no private right of action.
 - Who should be aware: NY-based entities and others who possess personal data from NY residents (particularly high volumes of sensitive data).

- NYDFS Cybersecurity Regulations (23 NYCRR Part 500) (“NY Cyber Regs”)
 - Outlines cybersecurity standards for financial companies in New York.
 - Companies must conduct risk assessments; maintain audit trails; dispose of data securely; limit access; develop a written cybersecurity policy; designate a Chief Information Security Officer; and abide by other best practices for cybersecurity.
 - Companies must report data security breaches to the Department within 72 hours of detection.
 - Who should be aware: Any entity regulated by the NYDFS.

State Biometric Laws

■ State Biometric Information Laws

- Illinois, New York, Texas, Vermont and Washington all have laws regulating the collection and use of biometric information.
- San Francisco, Oakland and Portland, and in Massachusetts, Boston, Brookline, Northampton, Springfield and Cambridge are among the cities that have banned the governmental use of facial recognition technology.
- Illinois' statute has a private right of action and is thus most prominent.
- Facebook recently settled a class-action suit under the Illinois BIPA for \$550M (face tagging).
- Even more state and local biometric information laws expected.

■ Will This All Be Superseded By Federal Legislation?

- Industry wants pre-emptive federal legislation.

Massachusetts Biometric Privacy Legislation

- In Senate Bill 2963, announced on December 1, 2020, there are proposed restrictions on the use of biometric surveillance by government entities in Massachusetts:
 - (b) Absent express authorization in a general or special law to the contrary, it shall be unlawful for a public agency or public official to acquire, possess, access, use, assist with the use of or provide resources for the development or use of any biometric surveillance system, or to enter into a contract with or make a request to any third party for the purpose of acquiring, possessing, accessing or using information derived from a biometric surveillance system.
- <https://malegislature.gov/Bills/191/S2963>
- Massachusetts Bill H.287 (and similar S.98) would amend chapter 93H:
 - To expand its scope to include “biometric indicators”
 - “Biometric indicator”: any unique biological attribute or measurement that can be used to authenticate the identity of an individual, including but not limited to fingerprints, genetic information, iris or retina patterns, facial characteristics, or hand geometry.

AI and Health Privacy/Privacy Rights

- Announced October 4, 2022, a Blueprint for an AI Bill of Rights:
<https://www.whitehouse.gov/ostp/ai-bill-of-rights/>
- There was a year of collecting public input that led to this document, including:

Panel 6: The Healthcare System. This event explored current and emerging uses of technology in the healthcare system and consumer products related to health.

Welcome:

- Alondra Nelson, Deputy Director for Science and Society, White House Office of Science and Technology Policy
- Patrick Gaspard, President and CEO, Center for American Progress

Moderator: Micky Tripathi, National Coordinator for Health Information Technology, U.S Department of Health and Human Services.

Panelists:

- Mark Schneider, Health Innovation Advisor, ChristianaCare
- Ziad Obermeyer, Blue Cross of California Distinguished Associate Professor of Policy and Management, University of California, Berkeley School of Public Health
- Dorothy Roberts, George A. Weiss University Professor of Law and Sociology and the Raymond Pace and Sadie Tanner Mossell Alexander Professor of Civil Rights, University of Pennsylvania
- David Jones, A. Bernard Ackerman Professor of the Culture of Medicine, Harvard University
- Jamila Michener, Associate Professor of Government, Cornell University; Co-Director, Cornell Center for Health Equity

Panelists discussed the impact of new technologies on health disparities; healthcare access, delivery, and outcomes; and areas ripe for research and policymaking. Panelists discussed the increasing importance of technology as both a vehicle to deliver healthcare and a tool to enhance the quality of care. On the issue of delivery, various panelists pointed to a number of concerns including access to and expense of broadband service, the privacy concerns associated with telehealth systems, the expense associated with health monitoring devices, and how this can exacerbate equity issues. On the issue of technology enhanced care, some panelists spoke extensively about the way in which racial biases and the use of race in medicine perpetuate harms and embed prior discrimination, and the importance of ensuring that the technologies used in medical care were accountable to the relevant stakeholders. Various panelists emphasized the importance of having the voices of those subjected to these technologies be heard.

New SEC Rules

- **Rule 10**
 - Imposes new cybersecurity requirements on “Market Entities,” and a subset of those entities defined as “Covered Entities”
 - Four major requirements
 - Cybersecurity policies
 - Notification and Reporting
 - Public Disclosure
 - Recordkeeping
- **Regulation SCI Amendments**
 - Expands the scope of entities covered by the rule
 - Adds a host of new requirements
- **Regulation S-P Amendments**
 - Incident Response Program
 - Customer Notification
 - Expands scope of covered information
 - Expands rule to transfer agents
 - Recordkeeping

What Disclosures do the SEC Require?

Governance and Oversight

- How the Board is informed of cyber risks and incidents.
- How the Board integrates cyber risk and incident response into its overall risk management framework

Risk Assessment and Management

- How management establishes and implements cybersecurity policies and procedures.
- Management's role and expertise in uncovering, assessing, and addressing cyber risks
- Incident response