Beyond California: State Standards for Privacy & Cybersecurity

Katherine Georger
Duke University Health System

David Behinfar
UNC Health Care System

Campbell Tucker
Novant Health

David Holtzman
CynergisTek

States Expanding Scope & Enforcement

Current State of Privacy

- HIPAA Privacy and Breach Notification Rules set bright line standards for most health care providers, insurers and vendors
- GDPR influencer of development of new federal and state privacy schemes but has had limited impact on U.S. healthcare organizations
- All states and territories have breach notification requirements to notify consumers when data compromised
- 22 states have laws that protect health information and personal information more broadly than HIPAA or other federal standards
- California to require businesses to give consumers notice and choice when personal information collected and shared

States Changing Definition of Health Information

- HIPAA applies to a defined set of information when created or maintained by a limited set of organizations
  - Covered Entities
    - Group health plans, insurers and other payers
    - Healthcare providers that bill Medicare, insurance & health plans electronically
    - Healthcare clearinghouses
  - Business Associates
    - Contractors & vendors of CEs who create, maintain or transmit PHI
- States broadly defining PII held by data owner or data processor

States Taking Enforcement Action

State attorneys general (AGs) are bringing enforcement actions to protect consumer information from unauthorized disclosure.

AGs in Massachusetts, New York, and New Jersey have been extremely aggressive.

Millions of dollars in settlements from healthcare systems and an assortment of IT services vendors for failing to safeguard data containing sensitive personal information.

PA Supreme Court found a Common Law duty to use reasonable safeguards to prevent its theft or unauthorized access.

50 Shades of Breach

- Research and review the laws in each state in which your organization does business or holds the PII of a state's residents.
  - How does that state define PII?
  - What is a "breach" and when is the breach reportable; who must receive notification; and, when must notifications be made?
  - What are the applicable state data protection or data disposal standards?
  - Are there industry specific cybersecurity program requirements (e.g. MI, MS, NY, OH, SC)?
  - How do state laws and requirements apply to 3rd party vendors when they maintain data PII?

Develop Situational Awareness

- Identify and inventory what PII is created, transmitted or maintained by, or on behalf, of your organization.
  - Include data in all forms and from any source (e.g. employees, patients or enrollees, online marketing, or website tracking).
  - What is the state of residency for each individual that has contributed PII?
  - It may be necessary to refer to state specific definitions of “what is PII?” to perform a complete inventory.

How State Laws Impact Research

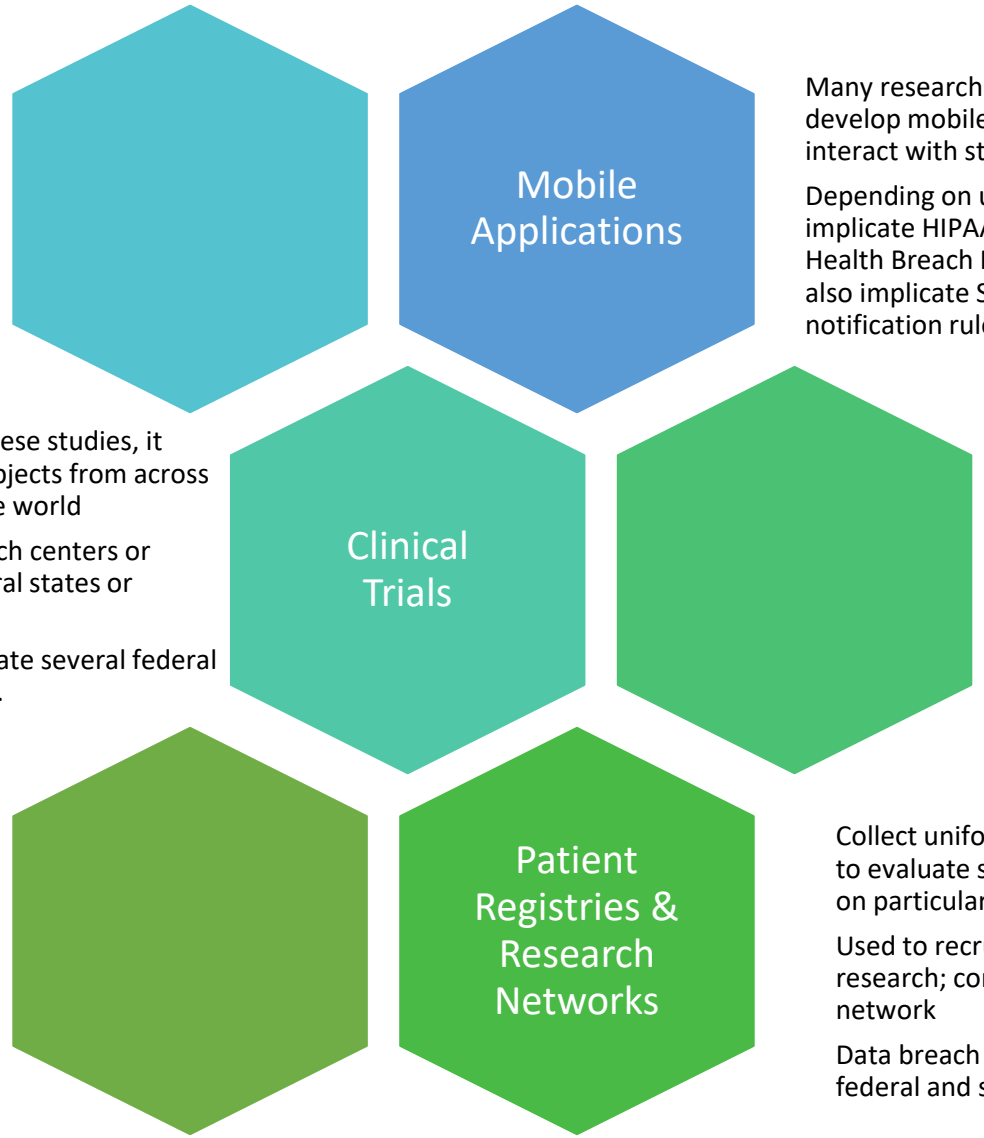
State Breach Laws & HIPAA

- The HIPAA Rules serve as the floor of privacy protections and preempts any *contrary* State law requirements, unless a specific exception applies:
  - State laws that are more protective of privacy rights;
  - State laws that mandate reporting of disease, public health surveillance, investigation, intervention; or
  - State laws that require health plan reporting.

State Breach Laws & Human Subjects Research

- *Collaboration/Multisite Studies*
  - Generally organizational IRBs have regulatory oversight responsibility for human subject research activities of their faculty, students, staff
  - Authorization/Collaboration Agreement (IAA/IIA/CIA) may cede regulatory authority as the IRB-of-Record to collaborating institution.
- *Single IRB of Record (sIRB)*
  - Two or more federally-assured institutions collaborate in human subjects research supported by a Common Rule agency (e.g., NIH), may rely on sIRB to avoid duplicate review.
- What impact does an IRB-of-Record or sIRB have on State breach notification obligations?

State Breach Laws & Human Subjects Research



Many research studies purchase or develop mobile applications to interact with study participants

Depending on use, purpose it could implicate HIPAA, FDA, and FTC Health Breach Notification Rule and also implicate State breach notification rules

Often by the nature of these studies, it leads to more diverse subjects from across the United States and the world

Can involve single research centers or multiple centers, in several states or countries

Data breach could implicate several federal or state notification laws.

Collect uniform clinical or other data to evaluate specific outcomes based on particular disease/condition

Used to recruit, monitor & develop research; connect into larger network

Data breach could implicate several federal and state notification laws.

Mixed Approach in the Carolinas

NC Becoming More Aggressive

- NC AG has become active in advocating for broader breach reporting and consumer data protection rights
  - Expanding definition of what is a breach
  - Adding medical information to definition of PII
  - Require reasonable security measures be in place to protect PII
  - Consumer right to accounting of PI compiled by a business
- Has participated with other AGs in settlements with Uber and Facebook over poor security and data sharing practices
- Joined 12 other states in suing Cloud EHR vendor MIE over security practices that resulted in a breach

NC Identity Theft Protection Act

- Unauthorized acquisition of computerized data that contains personal information
- Personal information defined
  - SSN, DL or other state issued ID #
  - Financial or credit card account # with any access code or PIN
  - Non-public information which may ID a person including biometric data
- Notification to individuals without unreasonable delay
- Required content of notice including advice for people who are affected on steps to protect themselves and how to contact credit reporting agencies
- Breaches require notification reporting to NC-DOJ Consumer Protection Division
- Compliance with state law is in addition to HIPAA
- Requirements for policies & procedures for destruction of sensitive information & electronic media

SC Insurance Data Security Act

- Implementation schedule staggered from 1/2019 – 7/2020
- Unauthorized acquisition of computerized data that contains personal information
- Notification to individuals without unreasonable delay
- Notification to SC DOI within 72 hours of cybersecurity incident
- Breaches >5000 require notification to credit reporting agencies
- Compliance with state law is in addition to HIPAA

SC Insurance Law Title 38 Chapter 99

- Cybersecurity Policies
- Designate CISO
- Enterprise-wide risk analysis
- Penetration testing and vulnerability assessments
- Audit trails to detect & respond to incidents
- Role based access privileges
- Evaluate, assess & test applications used on system
- Employ qualified cybersecurity personnel
- Set security standards for 3rd party vendors
- Use multi-factor authentication
- Limit data retention
- Train users & monitor activity
- Encrypt non-public information
- Have an incident response plan
- Annual certification and report incidents to SC DOI

SC Breach of Security of Business Data

- Unauthorized acquisition of computerized data that contains personal information
- Personal information defined
  - SSN, DL or other state issued ID #
  - Financial or credit card account # with any access code or PIN
  - Other non-public information which may be used to ID a person
- Notification to individuals without unreasonable delay
- Breaches >1000 require notification to credit reporting agencies & SC Department of Consumer Affairs
- Private right of action

California's New Privacy Act

California Consumer Privacy Act

- Goes into effect January 1, 2020
- Gives California consumers rights with respect to their personal information
- A consumer is defined broadly to include employees/families, prospective customers contacting us through their job, applicants for employment
- Applies to for-profit businesses with California presence that;
  - Have gross revenue in excess of $25 million; or,
  - Buy, receive, sell, or share for commercial purposes the personal information of 50,000+ California consumers, households, or devices; or,
  - Derive 50% or more of its revenues from selling personal information

4 Basic Rights Given to California Consumers

- The right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold
- The right to “opt out” of allowing a business to sell their personal information to third parties
- The right to have a business delete their personal information; and
- The right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

Healthcare Exemptions in CCPA

HIPAA COVERED ENTITIES

ENTITIES COVERED BY CALIFORNIA HEALTH CARE PRIVACY LAW (CMIA)

BUSINESS ASSOCIATES FOR ACTIVITIES COVERED BY HIPAA

NON-HIPAA COVERED PII HELD BY A COVERED ENTITY SAFEGUARDED TO SAME EXTENT AS PHI

UNDERSTANDING OF IMPACT IS EVOLVING

Compliance Challenges

- Assessing if your organization has a for-profit member or data controller in its family tree
- Identifying California residents
- Single national approach or California specific?
- Developing operations that can adjust for those residents who exercise rights
- Understanding what entities in health care and using health care information are covered or not


Questions?