HEALTHCARE PRIVACY AWARENESS

BEING PREPARED TO IMPLEMENT REGULATORY AND INDUSTRY CHANGES

NEHIA and HFMA Annual Compliance Conference
December 1, 2023

Presenter: Jennifer L. Cox, J.D.
Cox & Osowiecki LLC
Suffield, CT
jcox@coxlawoffices.com

Today’s Program

- Major shift in privacy and decision-making rights, targeted at reproductive health and gender affirming care
- Renewed focus on consumer data and privacy
- Next generation technologies, including Artificial Intelligence (A.I.)
- Reflections on the public health infrastructure post-pandemic

REPRODUCTIVE HEALTHCARE

Dobbs Replaces Roe v. Wade

- Dobbs v. Jackson Women’s Health Organization removes previously recognized constitutional right to privacy and bodily autonomy that had controlled U.S. law since 1973’s Roe v. Wade case
- Reproductive rights no longer have nationwide protection
- Abortion (and related issues) now legislated state-by-state

States Scramble to Revise Laws

- Legal protections in Roe v. Wade were based on privacy rights
- Once those rights were extinguished by Dobbs, the law returned to whatever was “on the books” in each state
- Many states had “old” laws on the books that did not reflect their current position
- Many states had bans or partial bans on the books that were idle

Immediate Operational Challenges

- Many prior laws and regulations are not based in current medicine or science
- Confusing and outdated terminology in laws
- Misalignment with standard of care: e.g., applying abortion bans to ectopic pregnancies or emergency medical care
- Providers (including pharmacies) in states with significant restrictions unable or hesitant to provide care

In Anti Abortion States

- Enacting significant limitations and/bans on abortion
- Making it a crime to perform an abortion
- Making it a crime to seek or have an abortion
- **Creating “bounty” laws**
- Creating laws to punish citizens who seek abortion outside of the state

In Pro-Choice States

- Revising existing laws and regulations to stabilize Roe status quo, removing artifacts of older laws
- Creating “shield” laws for providers
- **Addressing records privacy (harder than it sounds)**
- Restricting non-essential government access
- Attempting to counterbalance “bounty” laws

Many Areas Of Confusion

- Patients from out of state
- Medication assisted abortions
- Legal risks to licensed professionals
- HIEs, data sharing, patient consent for release of information
- Telehealth and mail order access

Complicating Factors

- Many new laws use the terminology: “Reproductive care”
- “Reproductive care” is a ***much*** broader category than abortion
- Gender affirming care being swept into restrictions and protections
- Federal guidance has been equivocal and sporadic; no clear path to a uniform set of laws at federal level

Operational Tips

- Carefully track the legal changes in reproductive care
- Review policies relating to:
  - Care delivery (do clinical staff understand the new environment; need training or info?)
  - Credentialing (reciprocal discipline in flux)
  - Graduate medical education
- Ensure record release policy, including handling subpoenas and government requests, tracks your (evolving) state law
  - Following HIPAA will not be enough

CONSUMER PRIVACY

Consumer Privacy

- Federal efforts to have a comprehensive, nationwide law for online consumer privacy have not been successful
- Since implementation of the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) other states have explored making their own consumer privacy laws
- These law usually focus on online services or cyber-based data, but affect all data media
- Having cyber services, and the internet, controlled state-by-state will be difficult to manage

Core Purposes Of Consumer Privacy Laws

- To give consumers control over whether their data should be used, including the consumer’s ability to:
  - Limit or direct uses
  - Opt out of use entirely
  - Force the holder of the information to destroy data
- To provide consumers with notice about how their data are being used

Consumer Privacy Laws v. HIPAA

- Often there are broad exemptions for HIPAA covered information in states’ consumer privacy laws
- Theory is that HIPAA already has a well-established privacy framework
- There is wide-spread scrutiny in consumer rights circles that HIPAA is too weak to deliver effective privacy
- Consumer privacy laws provide an individual more control over data about them than HIPAA does

Healthcare Affected By Consumer Privacy Laws

CAUTION!

- Exemptions for HIPAA data are generally **not sufficient to fully exempt a healthcare entity or provider** from consumer privacy laws, the line between the two worlds is *very thin*
- Geofencing, informational apps, social media, public facing websites, bulk data, portals, and data tracking can all result in identifiable data
- Technology can convert what looks like anonymized data into identifiable data (e.g., tracking technology and big data)

Operational Tips: Consumer Privacy

- Identify instances where HIPAA may not cover the entire data set or address all planned uses of the data
- Focus on the source of the data and whether HIPAA controls are applied
- Big data's "Tracking Data" – have a plan and response
- Marketing is a key focus area: consider whether purchased marketing lists (or fundraising lists) qualify as consumer data
- Check with community partners (those outside of HIPAA) whether their data sharing and handling is affected

EMERGING DISTRUST FOR TECHNOLOGIES

Reliance on Technology

- For a variety of valid reasons, providers and health insurers use and analyze data without express consent of patient/enrollee
- Providers and health insurers are encouraged to apply various technologies in innovative ways to:
  - Inform clinical decisions
  - Identify population and community health needs
  - Assist patients in finding resources
  - Avoid duplication of services
  - Create predictive analytics

Privacy Versus Data Use

- Privacy/patient control of their own data is at odds with flow of data and innovative uses of data
- Most recent example: the buzz around using artificial intelligence (A.I.) to help make healthcare decisions, or identify healthcare needs
  - Followed by an immediate call for laws to restrict the use of A.I.
- Are we at an industry turning point?

Bias In Technologies

- Growing focus on whether technologies create, perpetuate, and or worsen bias and/or discrimination
- Not entirely surprising that technology incorporates the biases inherent from programming and in baseline data
- Further struggle between predictive analytics at the individual patient level and generalizations about populations or groups
- False underpinning using race as a major reference point for clinical decisions: race is a social construct not a biological factor

Examples Of Bias Baked Into Technologies

- Pulse-Oximeters that are more accurate when used on light skin than dark skin
- Embedded racist pseudoscience incorporated into kidney function testing; reliance on social factors instead of biological factors
- Using predictive technology tools to make insurance coverage decisions for medical necessity based on an algorithm or software product (failing to assess at patient level)
- Using scoring analytics for organ transplant or crisis care
- Using predominantly male x-rays for training (skewing competency for future reads)

Operational Tips: Emerging Technologies

- Ensure “bias” discussion is ongoing and multidisciplinary
- Do not deploy A.I. (or any new predictive analytics) without some level of human oversight
- Consult bias guidance from FDA, The Joint Commission, other national organizations
- Increase and/or improve diversity and cultural bias training overall

COVID-19 RESPONSE:

FUTURE IMPACT ON PUBLIC HEALTH, DATA, AND TECHNOLOGIES

Public Health Activities And The COVID-19 Pandemic

- Generally agreed that the public health infrastructure (including data technologies and analytics staffing) was insufficient to handle the COVID-19 public health emergency (PHE)
- Numerous calls from all levels of organized medicine and other healthcare organizations to modernize the public health system, devote more resources to staff and technology, to have a better chain of command, and to collect more data routinely
- These calls to action are eerily similar to the time period immediately following the H1N1 PHE in 2009

Public Health Themes

- States’ immunization information systems needed upgrades
- CDC and HHS need more routine data collection
- Ongoing debate on how to limit medical misinformation
- Ongoing debate about privacy of government-obtained health information
- Outcomes were disproportionately worse for disadvantaged populations

Reality of Post-COVID PHE

- It is not feasible to operate in constant emergency mode; it’s inefficient and extremely expensive
- It’s impossible (or highly unlikely) we can guess what the next pandemic will be in a manner that allows for much preparation
- Data collection is EXTREMELY time-consuming despite advanced EMR technologies; virtually impossible for non-institutional or health systems to participate in sophisticated data collection
- Telehealth will expand
- Examination of policies and ethical considerations needed

Q & A