LEGAL AND REGULATORY CONSIDERATIONS IN THE US AND INTERNATIONALLY
Discuss the latest developments in the world of privacy and security, for the US and internationally
Discuss major areas of change over the next few years
Lessons learned from recent enforcement activity
Discuss the current enforcement environment at the state and federal level
Answer your questions about the future of healthcare privacy and security enforcement and related activity
GDPR

- Direct regulation – processors and controllers
- Transfer implications
- Contracting implications
GDPR

- Lots of nervousness
- Lots of uncertainty
- Expect “example” enforcement relatively early on (late 2018?)
- Expect contracting uncertainty
- There may be other changes as well
Privacy Shield/Data Transfer

- Aside from GDPR, some companies have to deal with Privacy Shield to become appropriate data transfer recipients
- Similar programs arising in other parts of the world (e.g., Asia-Pacific)
- Requires reasonable compliance activity
- Expect some enforcement in US
The New Administration

- We really know nothing about any intentions in the specific world of health care privacy and security
- Not a first, second or even third tier issue
- General consensus is that there are few strong policy positions beyond first tier issues and general philosophy
The New Administration

- Relevant philosophical points
- Overall concern about cybersecurity
- Willingness to engage in broad personal data review surveillance and oversight
- Presumably less government regulation
- Perhaps less governmental spending
- Perhaps less overall government enforcement
FTC Enforcement

- Wholesale change in Commission leadership (ongoing)
- Had been moving to a more aggressive view on “consumer harm” (with the likely reduction in enforcement)
- Will there be even less enforcement?
OCR Generally

- Two high level losses in main HIPAA enforcement leadership
- New OCR head with different priorities
- Real budget issues with a new (non-HIPAA) office added under same budget
- Recent reduction in enforcement, not clear if this is just transition
Changes to law/regulations

- Hard to see any push to change statutory language
- Unlikely to see new regulatory proposals, at least in early period (and likely longer)
- Unlikely to see pulling back on privacy rights
- Unlikely to see new HITECH rules that have been on hold (at least in short term)
Enforcement

- Enforcement certainly has been growing, but on a slow and steady basis
- Mainly growing because of low levels of enforcement activity in early years
- No particular reason to expect any fundamental change in enforcement philosophy
Enforcement

- Pending investigations take a long time to finish
- So no reason to think current staff won’t follow through to completion
- Future enforcement depends primarily on budget and resources more than philosophy
Enforcement

- Cases involving significant failures of compliance
- Cases involving repeated and/or uncorrected problems
- Particularly “noticeable” problems/High impact cases/send a message cases (?)
Business Associates

- Little real enforcement involving business associates yet
- A real challenge for OCR – how to treat companies who deal with much more than health care
- And the enormous range of size/sophistication of these entities
State Role

- Expect state AGs to be more active on privacy and security
- Some recent data breach cases where state AGs are aggressive (e.g., Equifax) or filling gaps (New York)
- Real questions as to whether they will understand/apply nuance or provide experienced judgment on HIPAA issues
Alternative enforcement

- The Plaintiffs’ Bar
- They are watching for openings because of damage theories AND exploring a broader role both in class action cases and in “sending a message” claims
The Plaintiffs’ Bar

- Looking for ways to avoid the need to prove specific damages
- Class action lawyers trying to define harm across all industries
- Portion of payments/premiums
- Overall weak security practices (anticipatory claims)
Damages are a Real Hurdle

- Smith v. Chase Manhattan Bank
- Financial institution gave list to third party, received payments on sales
- Said it didn’t do these things in privacy notice
- No damages alleged/no cause of action
- Only unwanted telemarketing
Smith v. Chase

“‘The ‘harm’ at the heart of this purported class action, is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm.’”
IoT and Unregulated Data

- Increasing concerns about big data environment
- Previous administration had been giving thoughtful and ongoing consideration to pros and cons of big data environment
- Those activities seem to have stopped for the time being
The biggest “next generation” issue

- HIPAA has always been a limited scope privacy/security rule
- It applies to healthcare information only where a covered entity is involved.
- Accordingly, there always have been gaps where various entities collect or maintain health care data but are not covered by the HIPAA rules.
The biggest “next generation” issue

- What is “outside” of HIPAA is growing
- Web sites gather and distribute healthcare information without the involvement of a covered entity.
- These range from commercial web sites (e.g., Web MD) to patient support groups to the growth of personal health records.
- Now add mobile apps. and wearables
More “next generation” issues

- An emerging (and related) issue - bringing “outside” HIPAA information “inside” HIPAA
- CEs are gathering all kinds of data about their patients/customers/insureds from outside the health care system and using it for “health care purposes”
Recent Headlines

- “Your Doctor Knows You’re Killing Yourself. The Data Brokers Told Her.” (Bloomberg)
- “You may soon get a call from your doctor if you’ve let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores.”
Recent Headlines

- Health plan prediction models using consumer data from data brokers (e.g., income, marital status, number of cars), to predict emergency room use and urgent care.
Tentative Predictions

- This HIPAA/non-HIPAA issue is not going away (although we may be on hiatus now)
- There is too much data being used by too many people in too many risky contexts
- Lots of pressure from many fronts to “do something” about this non-HIPAA health care data
Tentative Predictions

- 3 Main Options
- Something specific for this non-HIPAA health care data
- Something that covers all health care data
- A broader overall privacy law (with or without a HIPAA carve-out)
Legislation

- Expect state legislation on a variety of privacy and security topics
- Expect some pressure at federal level for data breach notification legislation or overall security legislation
- Don’t bet a lot of money on those passing
Keys for CEs/BAs

1. Risk Assessment
2. Risk Assessment
3. Risk Assessment
Other Keys

- Be responsive to any inquiries – thorough, timely, accurate
- Fix your problems – both immediate mitigation of breach-related issues and longer term process issues
- Make sure you have BA Agreements with everyone you should
Lessons Learned

- Be smart and careful about how you handle PHI
- Train your employees
- Be prepared to act quickly if there is a problem
- Have an overall risk assessment that incorporates your business activities
Questions?

For further information, contact:

Kirk J. Nahra
Wiley Rein LLP
202.719.7335
knahra@wileyrein.com
@kirkjnahrawork
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight