Emerging Regulatory Issues in Privacy and Data Security

13th Academic Medical Center Privacy & Security Conference

June 14, 2017
1. OCR Expectations

• Old news:
  ◦ Encryption
  ◦ Risk analysis, risk analysis, risk analysis
  ◦ Multi-million dollar settlements
  ◦ BAAs

• New news:
  ◦ Ransomware = breach; data integrity = harm?
  ◦ Operationalizing risk analysis results
  ◦ Refining organizational approach
  ◦ Victimhood is no defense
I HAVE A NEW HOBBY. IT'S CALLED PHISHING.

I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.

Sincerely,
I. B. Banker

Looks legit.
Enforcement Evolution

• Operationalizing Risk Analysis
  ◦ Children’s Medical Center Dallas - $3.2M
  ◦ Univ Mississippi Medical Center - $2.75M

• Refining Organizational Approach
  ◦ Failure to update BAAs: Woman & Infant Hospital of RI - $400,000
  ◦ Incomplete hybrid entity designation: U Mass Amherst - $650,000

• Victimhood Is No / Not Much Defense
  ◦ Memorial Health (FL): Employees steal data and commit fraud; failure to audit access exacerbates access - $5.5M
  ◦ Memorial Hermann Health System: Patient attempts fraud; health system subsequently IDs patient in press releases, posts info on website, and holds meeting with gov’t reps and advocacy group - $2.4M
Special Mention: OCR Math

- Ability to pay drives settlement; number of people affected does not
- Lack of security implementation (Children’s Medical Center Dallas)
  - Lack of safeguard $\times$ number of days = individual violations
  - Lack of policy $\times$ number of days = individual violations
- Impermissible disclosure
  - Number of people affected = individual violations
- Breach notification failure (Presence Health Network)
  - Each individual notice letter $\times$ every day late = individual violations
  - Media notice $\times$ every day late = individual violations
  - HHS notice $\times$ every day late = individual violation
- Aggravating factors (Children’s Medical Center Dallas)
  - Failure to address identified risks (repeatedly?)
  - History of non-compliance (multiple reported breaches)
2. FTC Enforcement

- **Old news:** Pursuing bleeding edge security matters
  - LabMD

- **New news:** Re-focus on consumer harm
  - Expect actions to follow actual breaches
  - Expect actions to follow actual data collection/disclosure inconsistent with privacy promises
  - Be aware of non-traditional sources of “breach reporting”
  - Expect more actions in health care space

- **BUT no jurisdiction over nonprofits**
Examples

• 2016 Testimony to Congress: Calls out wearables, apps, and PHRs citing lack of HIPAA coverage

• 2016 Practice Fusion: Cloud-based EHR solicited patients to review docs w/o full disclosure that reviews w/ treatment details would be public

• 2016 Henry Schein Practice Solutions: Provider of office mngt software for dentists falsely advertised HIPAA compliance and encryption

• 2015 PaymentsMD: Patient portal used to populate “Patient Health Reports”; clickthrough HIPAA authorization inadequate notice/consent

• 2015 IoT report: Suggests security risk analysis required

• 2014 GMR Transcription: File server exposed to Internet searches included clients’ patient data (audio and transcripts)

• 2014 Hosts seminar on consumer-generated health data: Explores data sharing by 12 popular health aps that share device and consumer IDs, exercise habits, and symptom searches with third parties
3. Expansion of State Breach Notification Laws

- **Old news:**
  - Apply based on person’s residency
  - Coverage of financial account details, SSN, and government-issued IDs

- **New news:**
  - More than a dozen address health and/or health insurance info
  - Several address biometrics
  - Increasingly cover hard copies
  - Increasingly lack a “harm threshold”
  - Increasingly apply limited HIPAA exceptions
  - Increasingly require notice to or consultation with state regulator
Examples / Considerations

- Florida covers name plus “any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis…”
  - Requires consultation with law enforcement to invoke harm threshold and notice to state regulator of determination if even one resident affected
  - HIPAA exception available but individual notice letter must be filed with state in addition to OCR

- Montana covers name plus information that “relates to an individual’s physical or mental condition, medical history, medical claims history, or medical treatment…”
  - Requires notice to state regulator if any Montana resident affected
  - No HIPAA exception

- Be careful in messaging and consumer protection offerings
  - May be evidence of harm/standing in subsequent lawsuits
4. State Privacy/Data Security Enforcement in Health Care

OUR FIREWALL IS DOWN. SOME BAD STUFF IS GETTING THROUGH.

HOW BAD?

SO FAR WE'VE SEEN VIRUSES, SPYWARE, TUBERCULOSIS, ZOMBIES, A DEPOSED DICTATOR, AND AN IPHONE 3GS.

BuRRRRR

UPDATE: AN ARMY OF MOLE PEOPLE FROM ANOTHER DIMENSION HAS TUNNELED THROUGH.

KEEP ME INFORMED.
4. State Privacy/Data Security Enforcement in Health Care

- Old news:
  - Individual state actions following data breaches
  - Multi-state pile-ons for controversial privacy practices (e.g., Google)

- New news:
  - Increasingly enforce HIPAA (e.g., CT, MA, MN, NJ, NY, VT)
  - Increasingly act in emerging health care space
Examples

• 2/2017: NJ settlement following “shadow IT” at Horizon Blue Cross
  ◦ Laptops used by marketing department stolen
  ◦ $1.1M settlement (HIPAA, NJ Consumer Fraud Act)

• 3/2017: NY settlement with three mobile health apps
  ◦ Misleading as to accuracy
  ◦ Failure to disclose that HIPAA would not apply (!)
  ◦ “Default consent” (use = agreement to privacy terms)

• 4/2017: MA settlement with digital ad company
  ◦ Geofencing used to direct ads based on proximity to reproductive health facilities and methadone clinics
  ◦ “Interfered with health privacy”
5. State Biometric Laws

I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES, AND I BRING YOU MY NEWEST BIOMETRIC SCANNER.

INSTEAD OF A PASSWORD, I PUT THIS ON YOUR HEAD AND SQUEEZE UNTIL YOU SCREAM IN A WAY THAT ONLY YOU CAN SCREAM.

NO, THAT'S NOT YOU.

GAAA!
GAAA!
GAAA!

DILBERT © 2007 Scott Adams. Used By permission of ANDREWS MCMEEL SYNDICATION. All rights reserved.
5. State Biometric Laws

• Old news: Illinois law
  ◦ Requires publicly accessible written policy; notice/consent requirement for collection/disclosure; prohibits “sell, lease, trade, or otherwise profit;” security; retention limit
  ◦ Private right of action

• New news:
  ◦ Texas – notice and consent to collect; prohibits “sell, lease, otherwise disclose;” security; retention limit
  ◦ Washington – notice/consent to collect, disclose, sell, rent; security; retention limit
    ➢ Exception: “federal health insurance privacy and portability act of 1996”
    ➢ Aka “HIPPA”
6. EU General Data Protection Regulation

• Old news:
  ◦ EU data protection law applies when “equipment” or “means” are used to collect data in the EU
  ◦ Broad definition of personal data
  ◦ Privacy principles
  ◦ Notice/choice
  ◦ Restricted transfers
  ◦ Consent, particularly for sensitive data
  ◦ Security
6. EU General Data Protection Regulation

- New news:
  - General Data Protection Regulation effective May 2018
  - Will apply based on offering products or services in the EU or monitoring behavior in the EU
  - Breach notification within 72 hours to lead DPA
  - Individual rights such as enhanced consent and access, data portability, “right to be forgotten”
  - Data protection officer
  - Data protection impact assessment/ “privacy by design”
  - Max fine up to 4% global revenue or 20
7. Text Message Lawsuits

• Old news:
  ◦ Class actions prevalent, large settlements follow
  ◦ Example: Walgreens $11M settlement for Rx refill reminders

• New news:
  ◦ Emerging case law suggest more favorable outcomes
  ◦ Zani v. Rite Aid – flu shot reminder
  ◦ Jackson v. Safeway – flu shot reminder
  ◦ Elkins v. Medco – medication therapy management
Questions?