Cyber Security Litigation Claims and Defenses

NCHICA 2016 AMC Security & Privacy Conference Series

June 27, 2016

Colleen Ebel, UNC Health Care

John M. Conley, J. Dickson Phillips, III, Mark A Hiller, Robinson Bradshaw

What If…

- A user at your medical center clicked a link in an email message to contact her email administrator about her over capacity email box so she would not lose her email. She was prompted to login and upon successful login with her medical center logon ID and password, she was happy to receive the message that her email box had been successfully expanded. She went about her business for the day.
- On her lunch hour she read a PHISHING SCAM alert in a special release of the employee news letter. She realized she had succumbed to the scam, and reported her transgression to the help desk, who immediately changed her password.
- Your privacy investigator learns the user is a medical school student in her clinical years. She reports she has PHI in her email.
- Your security investigation concludes there is no way to definitively know if the phishing attacker read mail, made a copy of the email box, or found and sent the PHI out of the mail system. Breadcrumbs for each of these email transactions can be removed. So while the security investigators could not find evidence that the attacker accessed or stole copies of private data, they also could not conclude that the attacker did not access or steal copies of private data.
- The privacy officer reports the breach to patients potentially exposed by this phishing

What If…

- Your security office implements a new malicious software detection security technology. It handles programs with viruses, worms and other malicious activity differently and more effectively than traditional antivirus software.
- Upon initial implementation, your new security appliance immediately picks up on suspicious traffic coming from 2 devices on your network and going to a command and control center (C&C) server on the Internet.
- The security investigation shows the devices are medical devices that are:
  - running an unsupported operating system. The medical device vendor still sells these devices and supports your installation of them, but does not offer an upgrade path.
  - not running antivirus software because it is not compatible with the operation of the medical device
  - not part of your vulnerability management program because the devices cannot tolerate a security scan without disruption
- The security investigation also shows the virus infection dates back 2 years, And while traffic was detected moving between the medical devices and the C&C server, content of the traffic was unknowable, and individual patient data exposure was inconclusive.
- You report the breach.

A not so uncommon theme to cyber breaches…

- Easy to find the evidence that a security breach has occurred.
- But often unable to definitively conclude that private data was actually exposed or copied without:
  - Extensive event logging not common in medical centers
  - Specialized tools and highly trained people on staff or a breach forensics company on retainer

HIPAA Privacy Rule

- When may a **covered entity** use or disclose **PHI**?
- Required disclosures
- Permitted disclosures (with and without authorization)
- Disclosures = Minimum Necessary
- Notice and administrative requirements
- Preemption of state law
- Breach Notification Rule – unsecured PHI

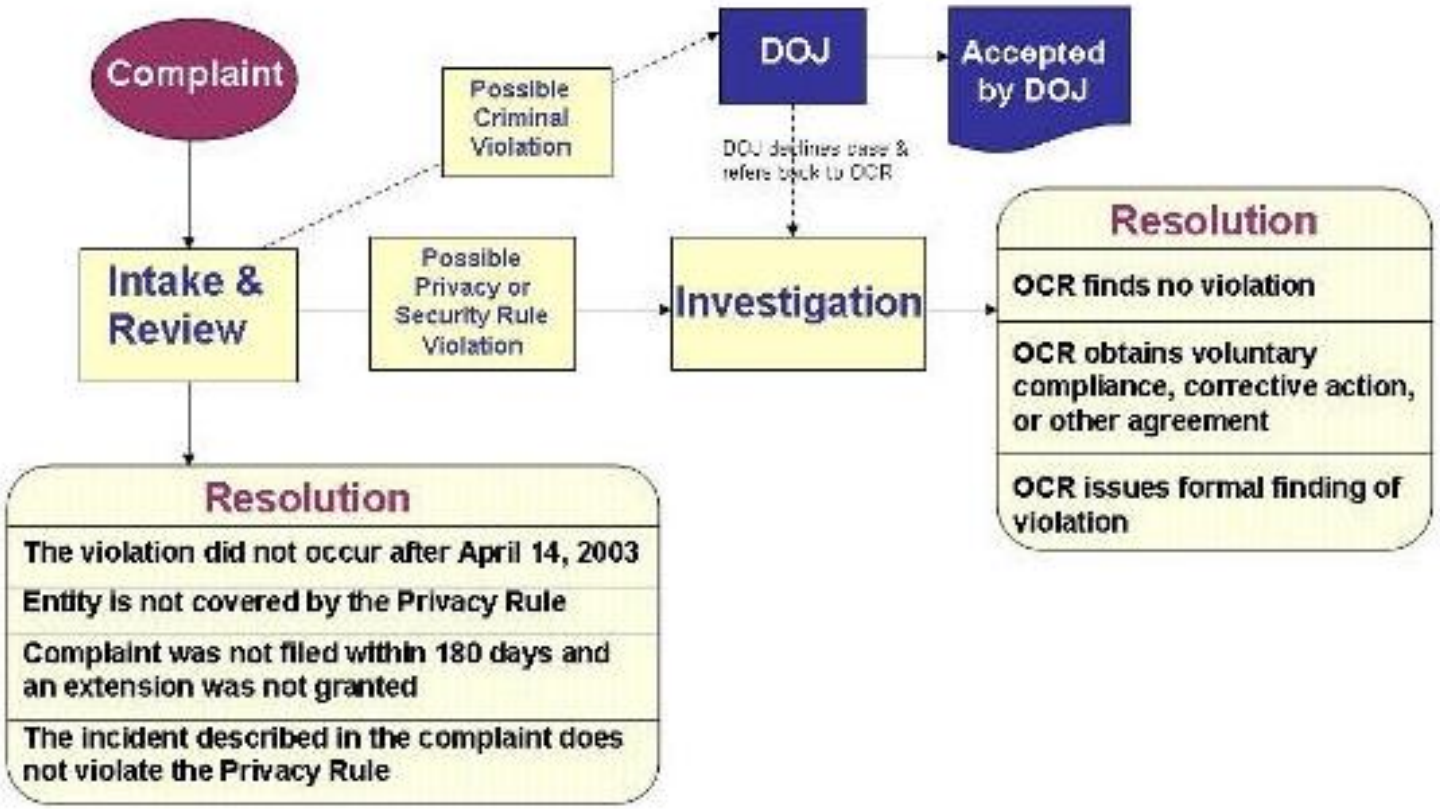
HIPAA Security Rule

- Covered entities must secure **e-PHI**
- General rule
- Flexible – “reasonably and appropriately” - does not require particular measures
- Risk analysis
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational requirements

Enforcement

- No private right of action
- Office for Civil Rights (HHS) – civil enforcement
  - Complaints
  - Compliance reviews
  - Education and outreach
  - Audits
- State Attorneys General – civil enforcement
- Department of Justice – coinvestigate complaints

HIPAA Privacy & Security Rule Complaint Process



Source: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

Civil Monetary Penalty

- Significantly harsher after HITECH Act (2009)
- Willful neglect = mandatory CMP (or settlement payment)
- Tiered penalty scheme
  - **Unknowing:** $100 to $50,000 per violation
  - **Reasonable cause**: $1,000 to $50,000 per violation
  - **Willful neglect – corrected:** $10,000 to $50,000 per violation
  - **Willful neglect – uncorrected:** At least $50,000
  - **Annual max:** $1.5M for identical violations in a calendar year
- Affirmative defense (if not willful) and waiver

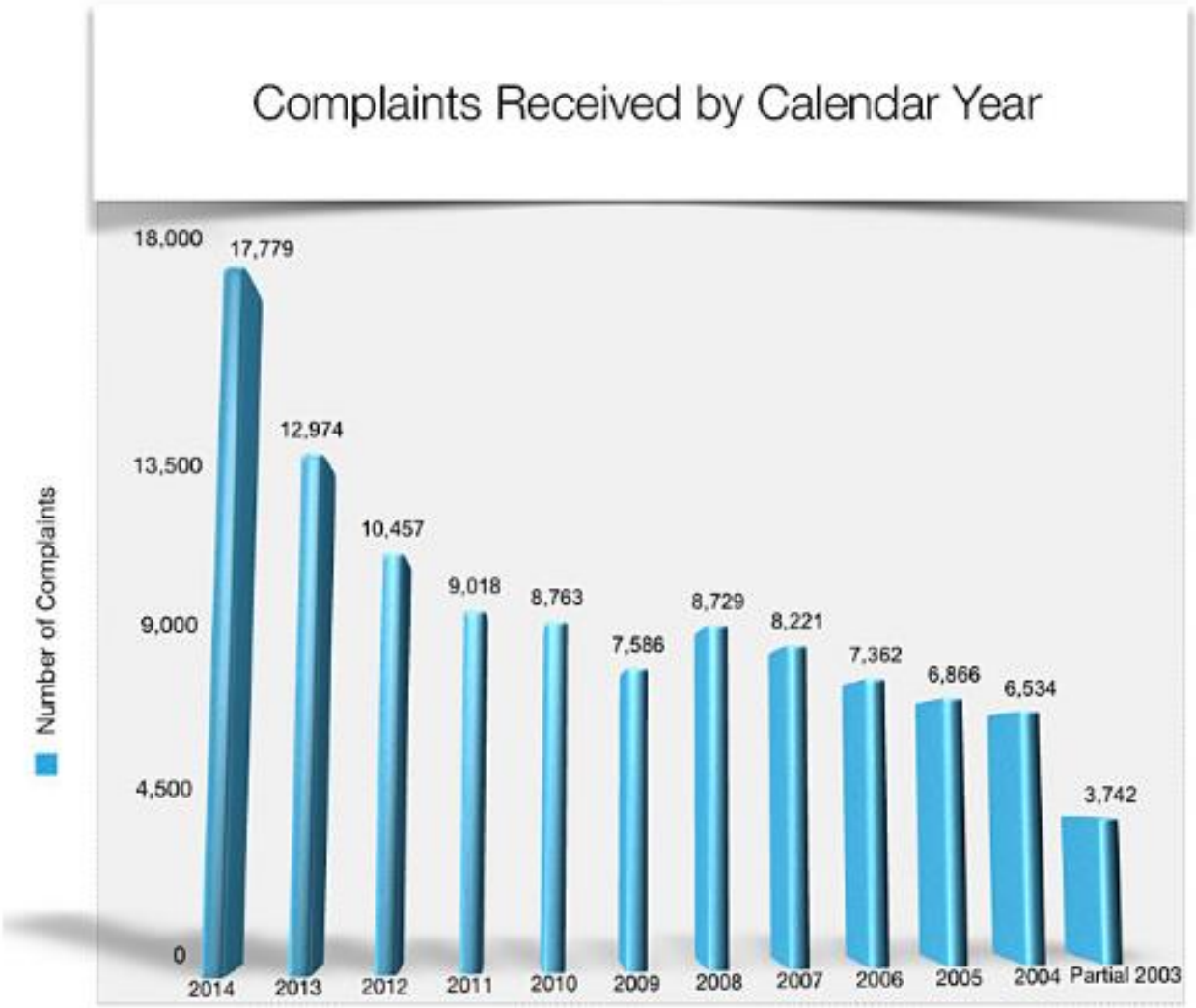
Enforcement Data

(As of May 31, 2016)

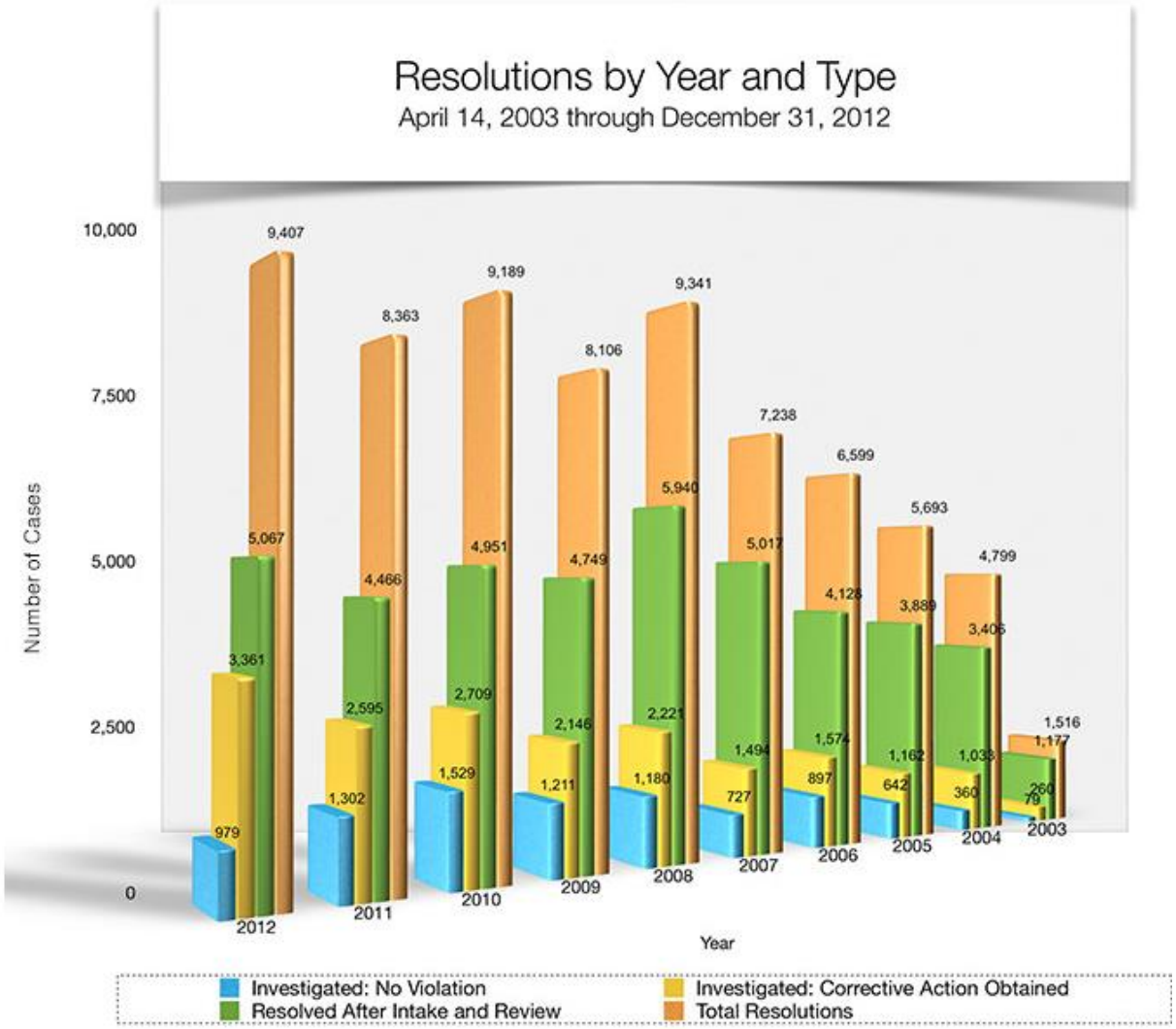
- Since April 2003: Resolved 128,872 complaints (96%)
  - 79,865 cases: Ineligible for enforcement
  - 13,748 cases: OCR early intervention/assistance; no investigation
  - 11,018 cases: Investigation → no violation
  - 24,241 cases: Investigation → corrective action or tech. asst.
    - **35 cases settled for total of $36.6M (in lieu of CMP)**

- Most common issues
  - (1) impermissible uses/disclosures of PHI; (2) lack of safeguards of PHI; (3) lack of patient access to PHI; (4) violation of minimum necessary rule; and (5) lack of safeguards for e-PHI

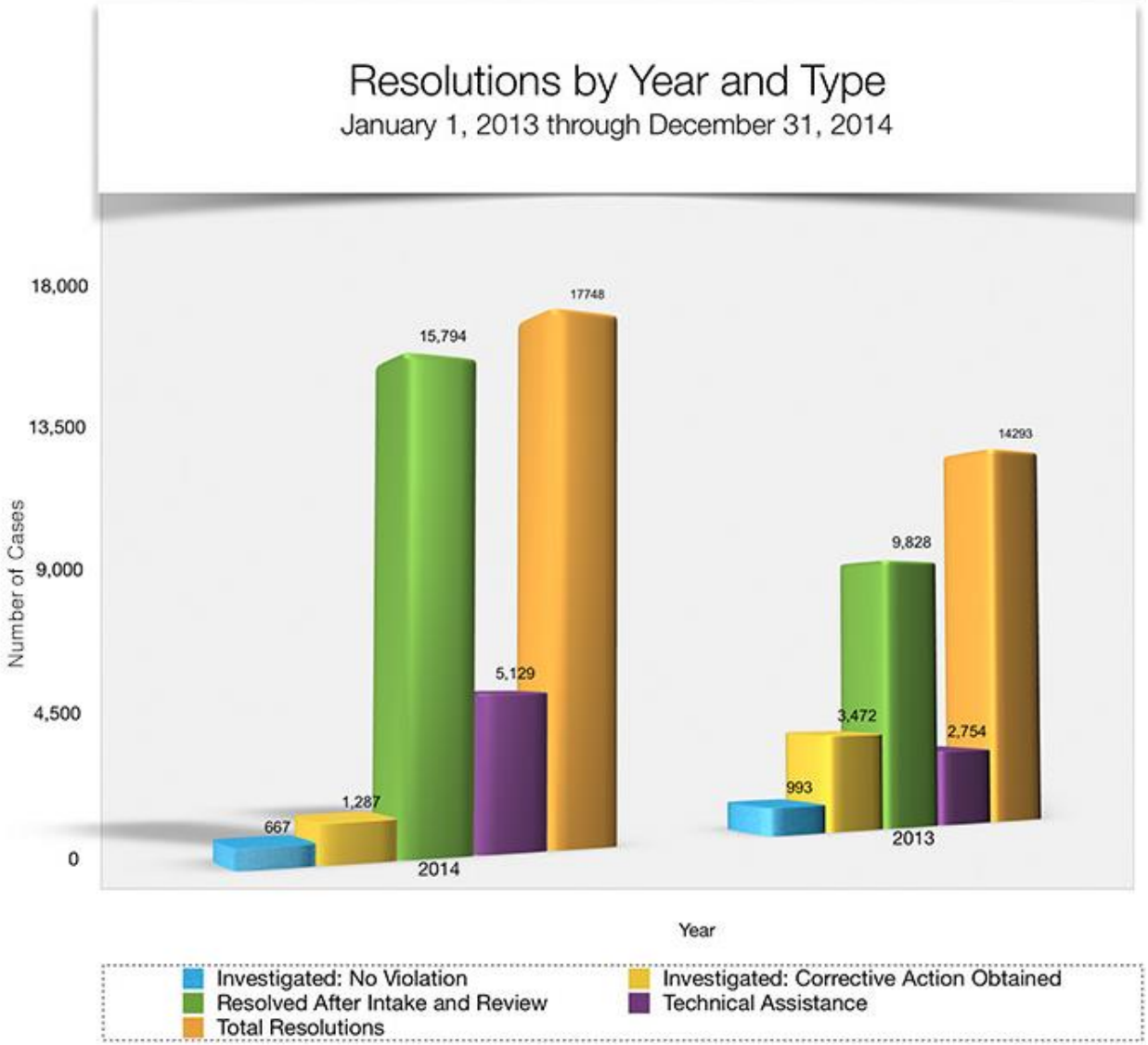
- Most common types of covered entities
  - (1) private practices; (2) general hospitals; (3) outpatient facilities; (4) pharmacies; and (5) health plans



Source: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html



Source: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#resol2014



Source: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#resol2014

New York Presbyterian Hospital
(April 2016 - $2.2M)

- "egregious disclosure" of PHI during filming of TV show "NY Med"
- NYP allowed TV crew to film patient who was dying and another patient in significant distress w/o authorization.
- Also failed to safeguard PHI and allowed film crew virtually unfettered access to facility
- Resolution agreement
  - $2.2M
  - CAP: Improve policies/procedures; notify HHS of p/p violations; implementation and final report to HHS
  - Term = 2 years

Feinstein Institute for Medical Research
(March 2016 - $3.9M)

- Laptop computer with e-PHI of approx. 13,000 patients and research participants stolen from employee's car
- Investigation began after Feinstein filed breach report
- Resolution agreement
  - $3.9M
  - CAP: Improve security management process and policies/procedures; training; notify HHS of violations; implementation and annual reports to HHS
  - Term = 3 years

University of Washington Medicine
(December 2015 - $750k)

- e-PHI of approx. 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware
- Information accessed: names, medical record numbers, dates of service, charges, address/phone, DOB, SS and insurance numbers
- UWM required its affiliated entities to have safeguards, but didn't ensure they conducted risk assessments and responded to vulnerabilities
- Resolution agreement
  - $750k
  - CAP: Risk analysis and risk management plan; reorganize compliance program; report violations; annual reports
  - Term = 2 years

New York Presbyterian Hospital and Columbia University
(May 2014 - $4.8M)

- Shared data network/firewall linking to NYP patients' e-PHI
- CU physician tried to deactivate personal computer server → e-PHI made accessible on Internet search engines
- Learned of breach by complaint from individual who found e-PHI of the individual's deceased partner (former NYP patient) on the Internet
- Resolution agreement
  - $3.3M (NYP) and $1.5M (CU)
  - CAP: Risk analysis, risk management plan, revising policies/procedures, training staff, and providing progress reports.

State Breach and Notification Laws

- 47 states and DC and PR have passed breach and notification laws
- Alabama, New Mexico and S. Dakota have not
- California first in 2003
- Laws generally protect personal information of a financial nature but may include “health information”
- Vary by triggering events and requirements upon happening of an event

Applicability of State Laws

- Generally apply to “personal information” of state’s resident regardless of where breach occurs
- if PI is also PHI, state law may nevertheless also apply because state law is not pre-empted by HIPAA
- provisos are (1) a number of state laws exempt HIPAA and (2) when both apply but requirements conflict, then only HIPAA is followed

Significant Elements of State Laws

- Definition of covered information
- Who must comply
- What is a breach
- Requirements for Notice
- Exemptions

Personal Information

- Generally the first name or initial and the last name of a person, plus
- additional identifying information that could be used for financial advantage, such as social security number, account numbers, credit card numbers, driver's license numbers
- NC has catchall of other information that could be used to access accounts
- laws often exempt encrypted or redacted materials

PHI as PI

- Some states define PI to include medical information
- California has a special medical information notification statute
- nearby states that include medical information include Virginia and Georgia

Breach

- Generally the unauthorized acquisition of personal information that may compromise the security, integrity or confidentiality of the information
- North Carolina and most states permit an analysis of whether any actual harm has or is likely to occur as a result of breach
- Unlike most, North Carolina defines breach to include paper records

Timing of Notification

- Generally, without unreasonable delay consistent with the needs of law enforcement
- Generally allow for investigation and assessment
- But some states have specific time requirements: E.g.: California, 5 days for medical information; Florida, 30 days; Conn., Ohio, Vermont, 45 days.

Method of Notification

- Default by mail
- Email allowed in a number of states on specific conditions
- Telephonic often permissible
- “substitute notification”, such as posting a general notice on a website, allowed in most states on certain conditions
- E.g. in North Carolina if the cost of regular notification would exceed $250,000.00 or the number of persons to notify exceeds 500,000
- Many require notice to the State Attorney General, including North Carolina

Contents of Notice

- Most statutes still do not contain specific requirements for content although increasing number do
- NC requires “Clear and conspicuous” notice including date and nature of breach, steps taken to minimize risk of further disclosure, and information on contacting the NC AG
- some require notice to credit agencies
- requirements for notice vary considerably and can require very particular information making a uniform notice impossible

Enforcement

- Criminal enforcement where there is criminal intent
- State Attorneys General civil enforcement in most states, lead to penalties and injunctions
- Private rights of action in a number of states: e.g. an unfair trade practice claim in North Carolina when there is actual injury
- Also, violations of state laws can lead to claims for negligence or breach of contract, or for claims of unfair or deceptive trade practices

Sources of Private Suits

- HIPAA and most state data laws ***don't*** allow for private suits (some state exceptions, especially CA & NY)
- Government enforcement only—but that can still lead to substantial fines
- So private suits based on ***common law—***typically negligence and breach of contract—and often state ***Unfair or Deceptive Acts or Practices*** statutes (like N.C.G.S. ch. 75)
- UDAP usually an add-on claim, requiring egregious misconduct
- HIPAA and state laws can set **standard of care,** violation of which can = negligence

Class Actions: Your Worst Nightmare

- A few plaintiffs represent thousands—or millions—of others in single, consolidated lawsuit
- The whole class wins or loses
- Financial damages usually awarded per formula or expedited proof process
- "Successful" consumer cases typically produce big attorneys' fees, little cash in the pockets of individual class members
- ***Certification*** is a critical preliminary step

Security Breach Litigation Profile

- About 4% of publicly reported security breaches result in class actions
- > 60% of those cases brought against ***retailers,*** though they account for only a small % of breaches
- Large majority of suits involve credit card data
- Most common legal theories are negligence, breach of contract, and UDAP
- So far, defendants almost always win, usually early in case—but hints that that's changing

Lessons from Financial Breach Cases

- Biggest problem for plaintiffs is ***plausibly*** alleging ***standing—***injury in fact
- Must show harm that is ***concrete and particularized*** and ***actual and imminent***, ***not conjectural or hypothetical***
- Courts evaluate ***speculative chain of possibilities,*** including intervening role of third parties—how much has to happen before harm can occur?

Lessons from Financial Breach Cases

- Lack of standing typically results in early dismissal
- Other problems for plaintiffs who survive standing--
- Proving that defendant was ***actually negligent***, or ***breached contract***
- Proving that they suffered ***financially compensable harm***—anxiety alone usually not compensable in ordinary negligence cases

The Standing Continuum

- ***Actual financial harm*** (e.g., fraudulent card charges, blocked access to accounts, late fees) ***usually*** confers standing
- ***Actual identity theft without financial harm*** (e.g., receiving targeted solicitations based on stolen info) ***sometimes*** confers standing
- The more specific and disturbing the evidence, the better for plaintiffs—e.g., military health data breach victims who get solicitations targeting their conditions have standing (*Science Applications Internat'l Corp.,* D.D.C. 2014), others don't
- ***Enhanced risk of future identity theft rarely*** confers standing—odds best for plaintiffs in 9th (West Coast) and 7th (Chicago) Circuits

Supreme Court Dodges Standing Issue: *Spokeo v. Robins* (5/16/16)

- Spokeo runs "people search engine" to provide info to prospective employers, etc.
- Robins claims S's profile of him reported false financial info, in violation of Fair Credit Reporting Act
- Lower court granted standing, based in part on alleged violation of federal statute

Supreme Court Dodges Standing Issue: *Spokeo v. Robins* (5/16/16)

- Supreme Court reversed and sent back for further consideration of standing issue
- Court ***might have*** decided whether alleging a violation of a federal statute (***HIPAA***, say?) by itself gives standing to victim
- But it didn't—instead, said lower court failed to consider whether plaintiff's injury was both concrete ***and*** particularized
- So case does little to clarify law of standing

Health Data Breach Cases

- Generally good news for defendants in few cases resolved so far
- ***Advocate Medical Group*** (Ill. App. 2015): state courts dismissed class action after theft of laptops containing SSNs and PHI of 4M+
- Allegations of risk of future harm are ***"merely speculative"***

Health Data Breach Cases

- Federal class action against ***CareFirst*** dismissed (D. Md. 5/16)
- "Unauthorized intrusion" into PHI database, beginning 6/14 and affecting 1.1M patients
- Risk of future harm ***"speculative,"*** depends on ***"chain of assumptions";*** court emphasizes that "***significant amount of time*** has passed" without actual injuries

Health Data Breach Cases

- But in 3/16 ***St. Joseph Health System*** settled CA state class action for millions
- St. Joseph allegedly exposed PHI of 31,802 patients on Internet
- Claims based on CA Medical Info Act, CA Unfair Competition Law, negligence—no available evidence of actual harm
- $7.5M to patients ($241 per!), $3M fund to cover future actual losses, $13M in remedial compliance initiatives, and—of course--$7.4M in attorneys' fees

Health Data Breach Cases

- Federal class action against ***Anthem Inc.*** survives motion to dismiss (N.D. Cal. 5/25/16)—case can proceed to discovery
- Hacker attack exposed PHI of 80M people
- Claims brought under ***CA state law***
- Anthem had previously sought—unsuccessfully—to access, image, and copy plaintiffs' devices to seek other causes of exposure
- Judge acknowledged novelty of legal issues

Practical Lessons from Cases

- ***Don't be negligent!***
- ***Seriously:*** Negligence requires failure to take reasonable care; scrupulous compliance with HIPAA and industry best practices make that hard to prove—you're not a guarantor
- ***Standing*** usually requires actual harm or imminent threat of harm
- So if something goes wrong, do what you can to ***minimize potential harm*** as soon as possible
- Unfortunately, no clear legal rules on ***how***—it's more of a technical question


ROBINSON
BRADSHAW