



Caught in the Middle Between Federal and State Breach Notification Requirements

HIPAA Summit XVIII

Jon Neiditz

jon.neiditz@nelsonmullins.com

(404) 322-6139

February 4, 2010

Nelson
Mullins

1. Why breach notification has been important, and what has been important about it
2. Challenges posed by HITECH breach notification requirements in light of lessons learned from 5 years of notification under state laws and other authorities
3. Fundamentals of risk mitigation strategy



- Breach Notification, rather than direct regulatory requirement, has since 2005 been the boiling water that led many a frog in diverse sectors to jump into better information security....
- For national health care organizations that limited their use of social security numbers, however, the water warmed gradually, as only a few states added medical information to notice-triggering personal information....
- Then came HITECH, and the health burner was switched up to a high boil....

Why did they jump?

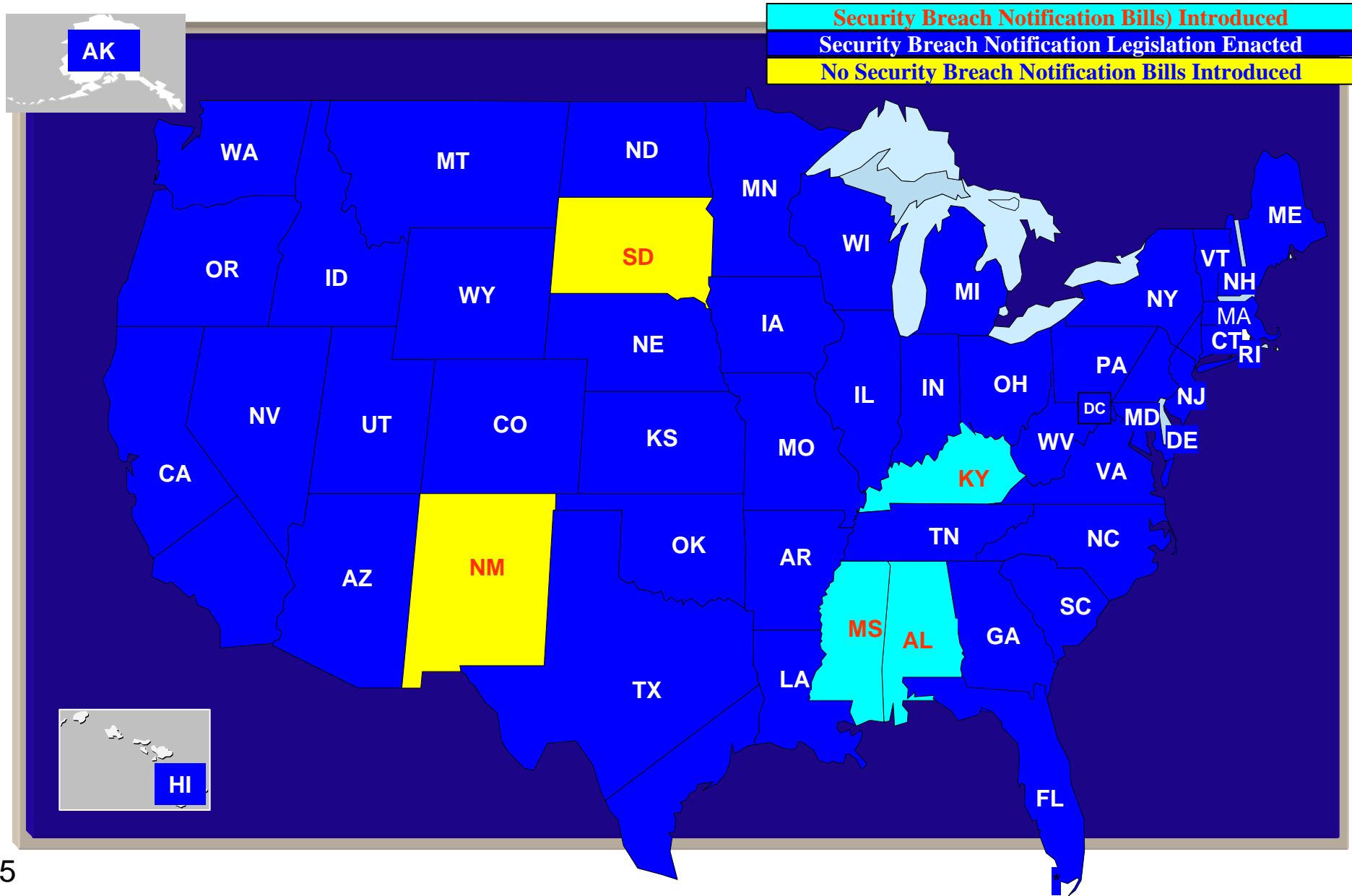


Nelson
Mullins

- Consumer businesses **may lose 20% to 30% of their customers** that receive breach notices from them:
 - Only 8% of consumers who receive a security breach notification did not blame organization that sent the notice (usually the “owner or licensee”)
 - Over 40% said they might discontinue their relationship
 - Another 19% said that they had already done so

Source: Ponemon Institute Surveys, 2005 and 2008 (30% is 2008 number)
- Higher percentage of **employee breaches** have been notice-triggering, due to:
 - More SSNs
 - More financial account information

The non-bank security breach landscape before HITECH



Things you ask at the time of the incident that produce varying results under various state laws

- Access, acquisition, risk of harm, use, illegal use, fraud?
- Encryption sufficient, or add requirement that it was in fact unused/unusable, or encryption not good enough?
- All businesses and agencies, or exclusions for privacy-regulated entities, or a narrower class?
- Non-electronic data included?
- Personal information: The original California list or up to ten additional elements?
- How soon must notification take place?
- Report to authorities required?
- Pre-breach measures required?
- Civil/criminal penalties and/or private right of action ?

The many gradations of "risk of harm" under federal and state laws

- HHS Rule: Even if acquisition, only notice-triggering if "risk of harm"
- FTC Rule: Rebuttable presumption that acquisition is access to notice-triggering information, and no harm or other requirement
- States: Many variants on:
 - access vs. acquisition vs. use
 - risk of harm
 - materiality
 - illegality
 - fraud



HITECH's completely new approach to notice-triggering information

State Model: "Personal information" means:

- an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 1. Social security number
 2. Driver's license number or California Identification Card number
 3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
 4. Up to 10 other factors added in many states

HITECH
Model:
ANY
"Unsecured"
Protected
Health
Information

Bold new worlds in definitions of "unauthorized"

- HHS: *Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule 
- FTC: *Unauthorized* means without the authorization of the individual 
- State law is much less specific, and can be so because the data elements are specifically defined

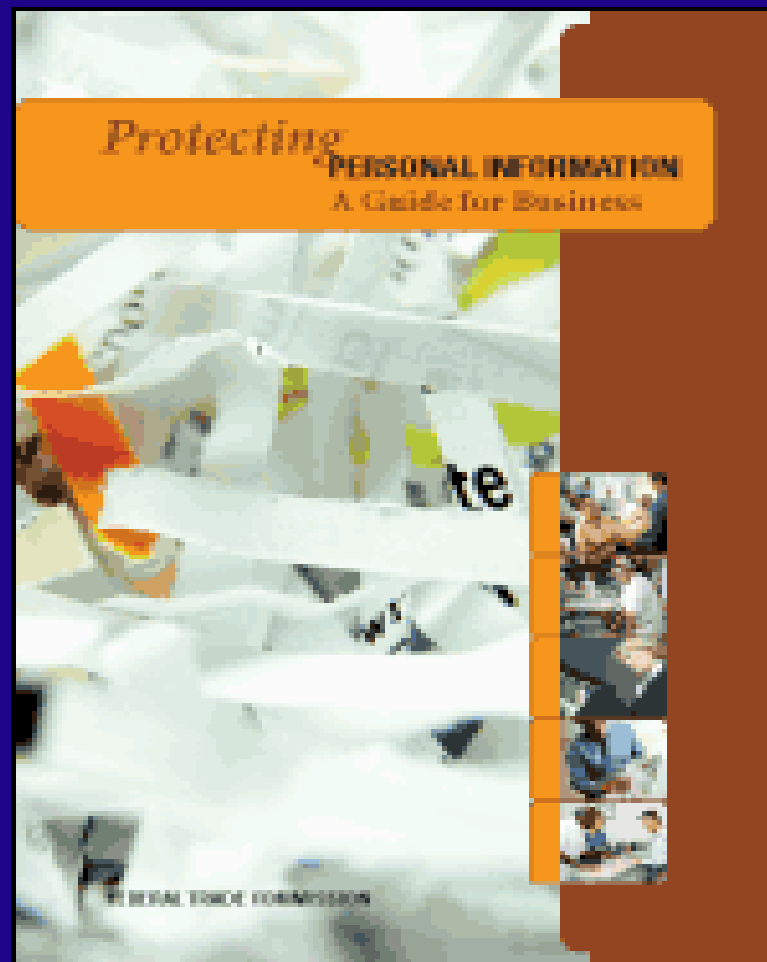
Encryption is not as "safe" a "harbor" as you have probably been led to believe

- HHS: *Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary ...
- FTC : *Unsecured* means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary
- Many of the states have turned away (in some cases explicitly and deliberately) from pure encryption safe harbor language to an apparent requirement that the encryption must have been effective, the key must not have also been breached, the information must be unusable, etc.
- Wyoming accepts only redaction

Unsettling encryption aside: Is the FTC an "encryption safe harbor" kind of place?

Like most sophisticated security schemes, the FTC emphasizes destruction at least as much as encryption:

1. Take Stock
2. Scale Down (i.e., destroy)
3. Lock It (i.e., encrypt)
4. Pitch It (i.e., destroy)
5. Plan Ahead



Unsettling aside 2: Payment Card Industry DSS – Encryption is not good enough for the dangerous elements; only destruction will do

		Storage Permitted	Protection Required	Encryption Required**
Cardholder Data	PAN	YES	YES	YES
	Expiration Date*	YES	YES	NO
	Service Code*	YES	YES	NO
	Cardholder Name*	YES	YES	NO
Sensitive Authentication Data	Full Magnetic Strip	NO	N/A	N/A
	CVC2/CVV/CID	NO	N/A	N/A
	PIN	NO	N/A	N/A

MUST KEEP

MAY NOT KEEP
(past problem areas)

- Data elements must be protected when stored in conjunction with PAN
- Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).



HHS, unlike PCI DSS, does not favor destruction over encryption, but....

- 2 approved methods for protecting: **encrypt** or **destroy**.
- 2 types of **encryption** specified: for data at rest (with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices) and for data in transit (those that comply with the requirements of Federal Information Processing Standards ("FIPS") 140-2).
- 2 methods of **destruction** specified: for non-electronic media, shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed, and for electronic, should be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.
- What is the legal consequence under the HHS rule if encryption as specified above does not in fact render the PHI "unusable, unreadable or indecipherable," and what does that mean for the supposed "safe harbor?"



- HHS Rule: YES
- FTC Rule: NO under the breach notification requirement, BUT dumpster diving cases have been among their most often pursued as unfair and/or deceptive trade practices (Section 5) (any personal information, almost any entities) and/or under the FACTA Disposal Rule (information derived from consumer reports only) since 2005
 - From *In Re Nations Title Agency* to *CVS Caremark* and more to follow
- 6 States: YES
- Other States/DC/Territories: NO

- HIPAA: Yes, but Security Rule applies only to **electronic PHI**
- FTC:
 - Safeguards Rule-level security required of all entities subject to Section 5 jurisdiction (unfair trade practices)
 - FACTA Disposal Rule only to consumer report information
 - Red Flags
- States: Complex and varying requirements around general security of personal information (at least 10 states), social security numbers (29 states), and secure destruction of personal information (23 states).

- HHS Rule: 60 days after reasonably should have known
 - Covered entities may be held to the date their business associate should have known if those business associates are agents under federal agency law 
- FTC: 60 days also, but notify the FTC in **10 business days** if 500 or more individuals affected 
- State Laws: 7 days after law enforcement in Maine, 45 days after reasonably should have known in Florida, Ohio and Wisconsin; otherwise construction of words like "prompt" and "most expedient"

Response planning is the real risk mitigation

- **Identify stakeholders**
 - Business Unit Representatives
 - Privacy Officer / Legal / Compliance
 - Information Technology;
 - Risk Management;
 - Disaster Recovery / BCP
 - Public Relations
 - Vendor Management
- **Establish analysis and communication protocols**
- **Evaluate vendors needs**
 - Technology – to handle technical forensics
 - Legal – to assist in determining notification obligations and drafting letters/call center script
 - Call Center – to handle inbound calls from victims
 - ID Theft Mitigation – including credit monitoring and other solutions
- **Remediation and recovery considerations**
 - Contractual indemnities
 - Insurance policies
- **Ensure the stakeholders have authority to act instantaneously**

- Breach notification and its legal requirements generally leave all the risk on the entity closest to the enrollee/patient relationship (covered entity, owner or licensee, PHR vendor), rather than on the "downstream" entities that just have to notify upstream
- You vendor must be required:
 1. to contact you when it first suspects that there may have been an incident, NOT when it has investigated or knows all of the employees whose information was breached
 2. To follow your instructions in connection with investigation and notification
 3. To assume financial responsibility, to the maximum extent possible, for all costs incurred associated with the breaches it has caused.
- Watch out, e.g., for:
 - vendors who may eat up your 60 days under the HHS rule
 - Vendors without good intrusion detection
 - Vendors whose uncritical use of public cloud computing undermines their intrusion detection and security

Be savvy about the security breach industry

- Many forensics firms, PR firms and credit bureaus offer products that bundle breach-related services
 - Be very careful about listening to any vendor that has a financial interest in notification or other services
 - Make sure you get a quick, independent read on legal requirements and whether and how notice should be given
- The great majority of breaches are not notice-triggering and may be addressed very quickly and inexpensively
- When breaches are notice-triggering, the quality of the communication matters
- Do not be misled about the value of notification or of credit monitoring to your patients, enrollees and employees
 - Negotiate credit monitoring in advance of breach and **for number of enrollees accessing the service, not number of records breached**
- Do not assume insurance coverage addresses your risks



Any questions?

Jon Neiditz

jon.neiditz@nelsonmullins.com

(404) 322-6139