

Medical Data Security Beyond HIPAA: Practical Solutions for Red Flags and Security Breaches

April 3, 2009

Jon A. Neiditz
Cynthia B. Hutto
Ross E. Sallade
Eli A. Poliakoff

Nelson Mullins Healthcare Information Management Initiative

**Nelson
Mullins**

Nelson Mullins Riley & Scarborough LLP

Copyright© 2009 Nelson Mullins Riley & Scarborough LLP

Why are We Here?

Big Changes in Healthcare Information Security

- Healthcare providers are encountering:
 - "Red Flags" requirements;
 - Security breach notification laws (all around the country) now in the Carolinas;
 - New and difficult Breach Notification provisions specific to healthcare in the National Stimulus Package (ARRA);
 - For example, Business Associates are now covered by the HIPAA Security Rule rather than just contractual provisions
 - PCI DSS and other private standards.

Red Flags Rule - Background

- FACTA (2003) modified the Fair Credit Reporting Act
 - FCRA primarily addresses background checks, patient credit checks and financial underwriting.
- Many provisions designed to address identity theft
- Red Flags Regulations
 - Proposed Rule (2006)
 - FTC, FDIC, Treasury, Federal Reserve, NCUA
 - Final Rule (2007)

Red Flags Rule – Background (Cont'd)

- Compliance Deadline (November 2008)
 - FTC compliance deadline for 'Red Flags' component delayed to May 1, 2009
 - FTC: healthcare providers, including institutions, practices, non-profits and governmental entities are not exempt
 - "Hospital" sign in FTC's Red Flags Guide
 - Address Discrepancy Rules: compliance deadline not delayed

Red Flags and Medical Identity Theft

- Unique concerns and threats
 - Patient safety
 - Patient financial considerations
 - Patient insurance ramifications
 - Provider liability considerations
- HIPAA's limitations

Red Flags Rule - Components

- Identity Theft ("Red Flags Rule")
- Card Issuer Duties
 - N/A for most of this audience
- Address Discrepancy Rule

Identity Theft "Red Flags Rule"

- "Red Flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft
- Applies to a creditor that offers or maintains covered accounts
 - Creditor:
 - Regularly extends, renews, or continues credit or regularly arranges for extension of credit
 - Credit = right granted to defer payment

Identity Theft "Red Flags Rule"

- "Covered Accounts"

Account offered or maintained primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions

OR

Account offered or maintained for which there is a reasonably foreseeable risk of identity theft to customers, or to the safety and soundness of your entity.

Account = continuing relationship to obtain a product or service for personal, family, household or business purposes.

Evaluate risk to you and your customer

Red Flags Rule - Requirements

- *Written Identity Theft Prevention Program*
 - Substantive Requirements
 - "Reasonable Policies and Procedures" to:
 - Identify relevant Red Flags and incorporate into Program
 - Detect Red Flags that have been incorporated into Program
 - Respond to detected Red Flags to prevent and mitigate identify theft
 - Ensure Program is periodically updated
 - » Program tailored to risks faced by organization

Red Flags Rule – Requirements (cont'd)

- Administrative Requirements
 - Board approval
 - Involve Board or senior management in development and implementation
 - Train Staff to implement Program
 - Appropriate oversight
 - Consider and incorporate as appropriate Guidelines provided in Appendix A and Supplement A to FTC Rules

Red Flags Rule – Penalties for Noncompliance

- Patient objections
- FTC enforcement actions/civil penalties
- Possible state tort claims

Practical Tips and Lessons Learned

- Incorporate into existing HIPAA/IT Security Program
- Identify Red Flags "areas" in the healthcare environment: generally areas of significant authentication risk, such as patient intake, identification confirmation, medical and billing records and collections
- Verify identity of persons opening accounts consistent with EMTALA

Practical Tips and Lessons Learned (cont'd)

- Isolated accounts or relationships
- Oversee service provider arrangements
- Appropriate risk management
- Identify appropriate responses to Red Flags: from records correction to police notification
- Educate staff and administration

Red Flags Program in Practice

1. Have your HIPAA Security and Privacy officials identify relevant patterns, practices, and specific forms of activity that should be treated as Identity Theft Red Flags in your operation.
2. Develop and adopt policies and procedures to detect Red Flags in areas such as patient intake, medical records and collections, as well as general policies concerning patient identification, verifying the validity of address change requests, etc.
3. Develop and adopt policies and procedures for incident response, such as monitoring patient medical and financial records for evidence of identity theft, contacting the patient, calling law enforcement, changing passwords, etc.

Red Flags Program in Practice (cont'd)

4. Have the Board or a committee of the Board adopt the program.
5. Make sure identity theft risks involving your vendors are addressed (including by assuring that they have their own Red Flags initiatives).
6. Update the program periodically based on lessons learned.

Address Discrepancy Rule

- Users of "consumer reports"
- Notice of Address Discrepancy
- Reasonable Policies and Procedures:
 - Reasonable belief that report relates to consumer for whom report is requested
 - Furnishing confirmed address for consumer subject to Notice of Address Discrepancy

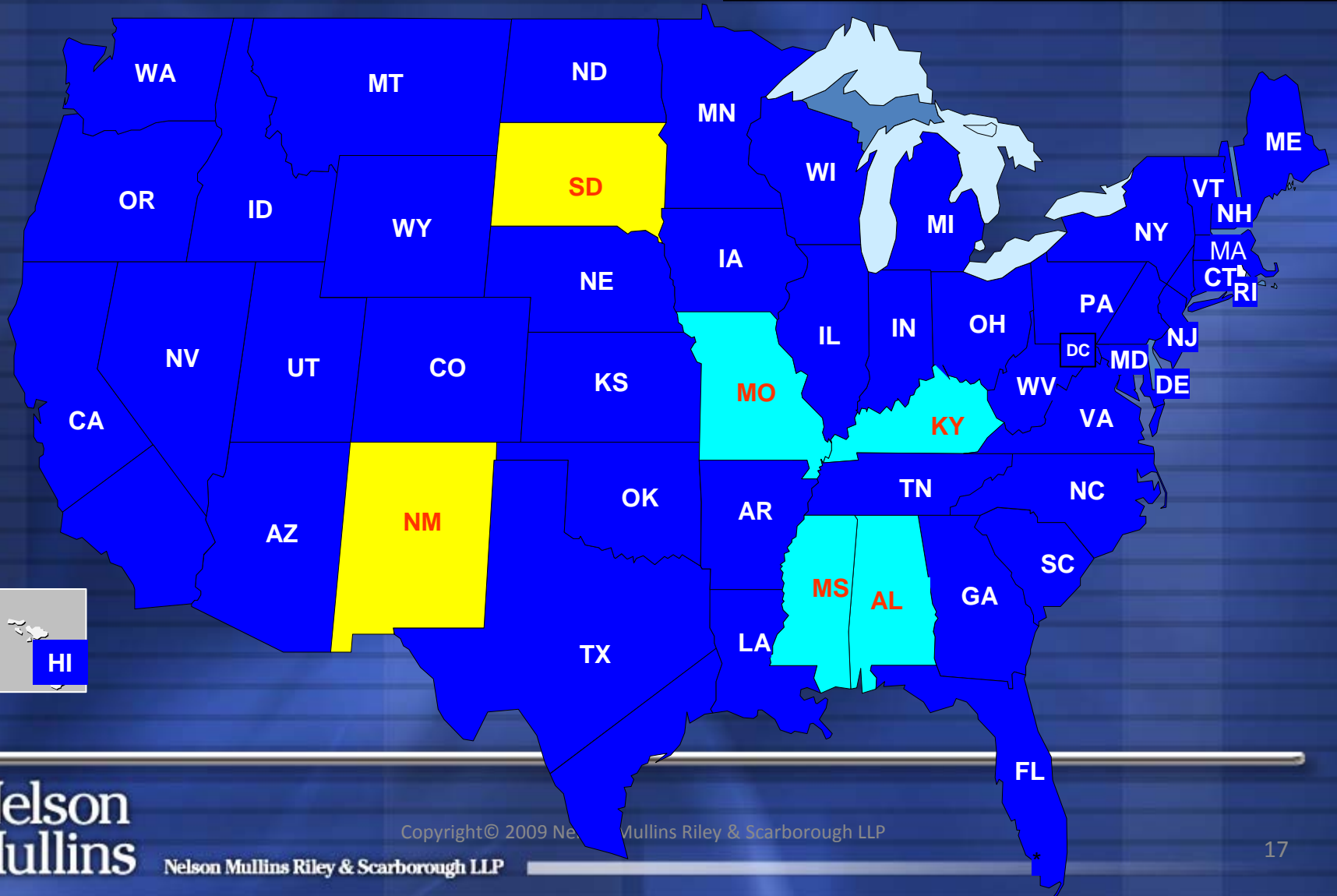
Security Breach Notification Requirements



Security Breach Notification Bill(s) Introduced

Security Breach Notification Legislation Enacted

No Security Breach Notification Bills Introduced



Some Important First State Law Questions in Dealing with Breaches

- Acquisition (or access) vs. harm
- All businesses vs. exclusions for privacy regulated entities or only “information brokers”
- Non-electronic data included?
- Personal information: The original California list vs. adding additional elements
- How soon notification must take place
- Report to authorities required?
- Law enforcement coordination exception?
- Pre-breach measures required?
- Civil/criminal penalties and/or private right of action

Law-Driven Business Crisis, Not Regulation, Drives Security

- B2C organizations like yours **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)
- Much higher percentage of employee breaches are notice-triggering
 - More SSNs
 - More financial information

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, expert 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 customers and employees
- Do not assume insurance coverage addresses your risks

South Carolina's Breach Law

- Effective 7/1/09
- Notice is triggered only when illegal use has occurred or is reasonably likely to occur or use of the information creates a material risk of harm
- In addition to the usual elements of notice-triggering information (name + SSN, driver's license #, account number + PIN), includes:
 - other numbers or information which may be used to access a person's financial accounts or
 - numbers or information issued by a governmental or regulatory entity that will uniquely identify an individual
- Exception for primary/functional regulator notification MAY exempt notification for patient – but not employee – breaches under ARRA
- Pre-breach measures include rules on disclosure of SSNs and secure destruction requirement
- Notice must take place in the most expedient time and manner possible and without unreasonable delay
- Private right of action
- Must inform Consumer Protection Division of Dept. of Consumer Affairs & all national Consumer Reporting Agencies if notifying 1,000+ persons

North Carolina's Breach Law

- Illegal use/harm threshold the same as SC
- Breach of **paper** documents clearly included
- In addition to usual elements of notice-triggering information includes:
 - checking or savings account #
 - credit or debit card #,
 - PIN,
 - digital signature,
 - biometric data,
 - fingerprint or
 - passwords
- Notice-triggering information also includes electronic ID #, email names or addresses, parent's maiden name or any other #s if they permit access to financial resources
- Pre-breach measure requirement excludes entities covered by GLBA, FCRA and HIPAA
- Private right of action if injured
- Report to Consumer Protection Division of Attorney General's Office and Consumer Reporting Agencies if notifying 1,000+ persons



ARRA 2009

- Breach notification obligations turning on "unsecured PHI"
 - Paper and even oral breaches (apparently) included
 - Exceptions
 - 60-day outside limit for notifications, but should be more prompt in the absence of justification
 - DHHS must be notified for breaches involving more than 500 people
- Expansion of HIPAA Security to all business associates
- Secretary of DHHS to issue annual guidance on technical safeguards
- Enforcement by state AGs, more stringent remedies and shift in burden of proof

Other Trends and Requirements

- State social security number protection, use and disclosure laws have also spread like wildfire (including to GA, NC and SC), and impact your employee side where HIPAA did not
- Secure destruction laws, including that FACTA Disposal Rule and state laws (including in GA, NC and SC) govern the destruction of both paper documents and electronic data containing personal information
- Watch for more specific and possibly non-technology-neutral refinements of "secured" or "encryption" under ARRA

Questions?

Nelson Mullins Riley & Scarborough LLP

Jon A. Neiditz

404.322.6139 • jon.neiditz@nelsonmullins.com

Cynthia B. Hutto

843.720.4307 • cindy.hutto@nelsonmullins.com

Ross E. Sallade

919.329.3875 • ross.sallade@nelsonmullins.com

Eli A. Poliakoff

843.534.4122 • eli.poliakoff@nelsonmullins.com