SECURITY BREACH RESPONSE

To Notify Or Not To Notify Is No Longer The Question

Robin Campbell
Chandra Westergaard

HOOPS2008
Crowell & Moring LLP
## States With Notification Laws

<table>
<thead>
<tr>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska</td>
</tr>
<tr>
<td>Arizona</td>
</tr>
<tr>
<td>Arkansas</td>
</tr>
<tr>
<td>California</td>
</tr>
<tr>
<td>Colorado</td>
</tr>
<tr>
<td>Connecticut</td>
</tr>
<tr>
<td>Delaware</td>
</tr>
<tr>
<td>District of Columbia</td>
</tr>
<tr>
<td>Florida</td>
</tr>
<tr>
<td>Georgia</td>
</tr>
<tr>
<td>Hawaii</td>
</tr>
<tr>
<td>Idaho</td>
</tr>
<tr>
<td>Illinois</td>
</tr>
<tr>
<td>Indiana</td>
</tr>
<tr>
<td>Iowa</td>
</tr>
<tr>
<td>Kansas</td>
</tr>
<tr>
<td>Louisiana</td>
</tr>
<tr>
<td>Maine</td>
</tr>
<tr>
<td>Maryland</td>
</tr>
<tr>
<td>Massachusetts</td>
</tr>
<tr>
<td>Michigan</td>
</tr>
<tr>
<td>Minnesota</td>
</tr>
<tr>
<td>Montana</td>
</tr>
<tr>
<td>Nebraska</td>
</tr>
<tr>
<td>Nevada</td>
</tr>
<tr>
<td>New Hampshire</td>
</tr>
<tr>
<td>New Jersey</td>
</tr>
<tr>
<td>New York</td>
</tr>
<tr>
<td>North Carolina</td>
</tr>
<tr>
<td>North Dakota</td>
</tr>
<tr>
<td>Ohio</td>
</tr>
<tr>
<td>Oklahoma</td>
</tr>
<tr>
<td>Oregon</td>
</tr>
<tr>
<td>Pennsylvania</td>
</tr>
<tr>
<td>Puerto Rico</td>
</tr>
<tr>
<td>Rhode Island</td>
</tr>
<tr>
<td>South Carolina</td>
</tr>
<tr>
<td>Tennessee</td>
</tr>
<tr>
<td>Texas</td>
</tr>
<tr>
<td>Utah</td>
</tr>
<tr>
<td>Vermont</td>
</tr>
<tr>
<td>Washington</td>
</tr>
<tr>
<td>West Virginia</td>
</tr>
<tr>
<td>Wisconsin</td>
</tr>
<tr>
<td>Wyoming</td>
</tr>
</tbody>
</table>
Basics

• Generally requires notification in the event of “an unauthorized access to or acquisition of unencrypted, computerized data”

• Basic definition of personal information: First name or initial and last name, plus
  – SSN
  – DL number or state ID number
  – Account number, credit or debit number plus security code, access code, or password
Pre-breach measures

Similar to HIPAA Security Rule requirements

• Reasonable and adequate security procedures

• Contractual safeguards for transfers

• Effective and timely document destruction methods and policies

• Encryption for transfers

Look out for Massachusetts style regulations
Difficulty Lies in the Differences

Definition of PI

- Items added by other states:
  - DOB
  - Employer ID
  - Account numbers without codes/PINs
  - Taxpayer ID
  - Any government issued ID
  - Medical information
  - Health insurance information
  - Mother’s maiden name
  - Digital signature or biometric data
  - Tribal ID

If one state definition triggers notification, difficult not to notify in all states affected.
Paper Versus Electronic

Paper States
• Alaska
• Connecticut
• Hawaii
• Indiana
• Massachusetts
• North Carolina
• Wisconsin

Paper for pre-breach
• CA, MD, NJ, UT, VT
Encrypted Data Included

- Louisiana
- Maryland
- Wyoming

Others only include it if encryption key has been compromised as well.
Whom To Notify

- Authorities
  - Delaware
  - Hawaii
  - Maine
  - Maryland
  - Massachusetts
  - New Hampshire
  - New Jersey
  - New York
  - North Carolina
  - Puerto Rico
  - South Carolina
  - Virginia
- Before or after notice to individuals
  - New Jersey, Maryland—prior to notifying individuals
  - Puerto Rico—within 10 days
What To Say

• Content requirements
  – Hawaii
  – Iowa
  – Maryland
  – Massachusetts
  – Michigan
  – New Hampshire
  – New York
  – North Carolina
  – Oregon
  – Puerto Rico
  – Vermont
  – Virginia
  – West Virginia
  – Wisconsin
  – Wyoming

• Conflicting requirements
  – Massachusetts versus everyone else
When To Notify

Owner versus non-owner/vendor
• 45 days owner to individual: FL, OH, WI
• 10 days non-owner to owner: FL
• 10 days to Dept. of Consumer Affairs: PR

Required versus recommended
• Required: 45 days/10 days
• Recommended: CA 10 days to individual
• Contractual: lots of variation
What You Must Provide

• Credit Monitoring Not Yet Legally Required--AGs/Govs pushing
• Call center/800 number
  – Vermont
  – Virginia
  – Wyoming
• Fraud alert assistance
  – Most states with content requirements require information on how to obtain, but do not require that company assist
Prevention

- **Inventory personal information**
  - What do you have and where is it?

- **Assess vulnerability to breach**

- **Benchmark current security against new standards**

- **Consider alternative use or elimination of personal information and don’t collect it unless absolutely necessary**
Prevention, continued...

- Limit access to personal data
- Utilize adequate administrative, technical and physical security safeguards, follow your own policies and procedures
- Train, Train, Train, not just on privacy and security, but recognizing breach
- Require adequate security of third parties through contract
  - Update existing business associate agreements?
  - Does it include a notification requirement
  - Indemnification in the event of a breach?
  - Know your contractual obligations with respect to security breach?
- Use intrusion-detection technology to rapidly detect breach
- Dispose of personal information in an effective and timely manner
Response

Incident Response Plan

- SIRT
- Templates
- Entities that have already been vetted
- Critical contracts, notification deadlines
- Contact lists: SIRT, Vendors, Clients
- Escalation plan, often turns into a business, not legal, decision
Response

- Secure the information/systems
- Conduct investigation
- Involve law enforcement
- Categorize data lost
- Document incident and response
- Be prepared with public statement
- Be consistent in statement, policy, practices
- Prepare for inquiries (policies, contracts, audits)
- Letters to individuals
- Letters to authorities
- Letters to CRAs
- Call Center FAQs/Call Script
- Vendor: Credit Monitoring, Notification
What’s Next

• Encryption for transfers: Nevada 08
• Encryption: Massachusetts rules
• General EU style requirements: Massachusetts rules
• Liability for costs by statute: retailers still the target
Interplay with HIPAA

- HIPAA does not require notification of affected individuals in the event of breach.

- However, unauthorized disclosure of PHI must be included in any accounting requested by the individual.
Implications for Government Contractors

- Medicare Advantage and Part D Contractors
  - CMS is concerned about potential identity theft affecting Medicare beneficiaries.
  - Contractors are required to notify CMS immediately upon discovery of any security breach compromising beneficiary personally identifiable information.
  - CMS will conduct a risk assessment to determine the plausibility of identity theft when a data loss or breach occurs.
Implications for Medicare Advantage and Part D Contractors, continued...

- Per CMS, there is a reasonable risk of identity theft if data includes
  - a SSN; or
  - the name, address, or telephone number along with an identification number, an account number, or any additional specific factor that could lead to the personal identifying profile of an individual.

- Depending upon the circumstances CMS may require
  - Notice to affected members
  - One year free credit monitoring
Implications for Government Contractors, continued...

• FEHBP Contractors
  – Any breach of security in FEHB enrollee data is considered a “significant event” that must be reported within 10 days of learning of the breach
  – OPM wants contractors to e-mail their Contract Specialists and Contracting Officer immediately in the event of a data breach or a suspected data breach involving FEHB enrollees
Implications for FEHBP Contractors, continued...

– Unlike HIPAA, contractors must notify affected FEHB enrollees of the breach within 10 days, including
  
  • A letter detailing the incident
  • A description of the types of personal information involved
  • The contractor’s efforts to investigate, mitigate, and protect
  • The contractor’s contact information and processes
  • Steps individuals should take to protect against identity theft

– Contractors must provide one year free credit monitoring
Other Implications for Government Contractors

- Sanctions for noncompliance including:
  - Monetary penalties
  - Suspension of enrollment
  - Suspension of payments

- Termination of Key Subcontract

- Termination of Contract
Federal Enforcement

• Since April 2003, DHHS has received over 38,812 HIPAA Privacy complaints. Over 80% of complaints received (over 32,232) were resolved through:
  – Investigation and enforcement (over 6,985);
  – Through investigation and finding no violation (3,467); and
  – Through closure of cases that were not eligible for enforcement (21,780).

• The compliance issues investigated most are:
  – Impermissible uses and disclosures of protected health information;
  – Lack of safeguards of protected health information;
  – Lack of patient access to their protected health information;
  – Uses or disclosures of more than the Minimum Necessary protected health information; and
  – Lack of or invalid authorizations for uses and disclosures of protected health information.
Federal Enforcement, continued...

- July 15, 2008 – DHHS enters into first-ever Resolution Agreement with a Covered Entity
  - Incidents involved lost and stolen backup tapes, optical disks, and laptops, containing unencrypted electronic PHI of over 386,000 patients.
  - $100,000 fine
  - Corrective Action Plan requiring the covered entity to:
    - Revise policies and procedures regarding data safeguards, off-site transport and storage of electronic media containing patient information (policy revisions subject to DHHS approval);
    - Workforce training;
    - Audits and site visits of facilities; and
    - Submission of compliance reports to DHHS for 3 years.
Questions?

Robin Campbell
(202) 654-6732
rcampbell@crowell.com

Chandra Westergaard
(202) 624-2584
cwestergaard@crowell.com