POST & SCHELL, P.C.
ATTORNEYS AT LAW

Hackers, Slackers & Packers: Preventing Data Loss & Dealing with the Inevitable

Steven J. Fox (sjfox@postschell.com)
Peter D. Hardy (phardy@postschell.com)
Robert Brandfass (BrandfassR@wvuh.com)
(Mr. Brandfass is General Counsel for West Virginia University Hospitals)

Data Breaches Are All Too Common

- University of Utah: back-up records of over 2 million patients were stolen in Summer 2008; included social security numbers of approximately 1.3 million people treated over many years
- University of Kentucky: disclosed in May 2006 that it inadvertently had posted about 1,300 social security numbers of its employees on a public Web site
- University of Virginia: laptop stolen in April 2008 from an employee contained sensitive information regarding more than 7,000 students, staff and faculty

Widespread Use of Information Technology Feeds Risks of Data Losses and Theft

- Sheer volume of computerized information acquired and maintained by colleges and universities is enormous
- Many different ways for breach to occur
  - Purposeful and malicious accessing
  - Misplacing laptops or disks
  - Accidental on-line exposures
- Federal Register: "[c]omputer systems at colleges and universities have become favored targets because they hold many of the same records as banks but are much easier to access."

A Web of Overlapping Data Privacy Protection Statutes and Regulations

- Gramm-Leach-Bliley Act ("GLBA")
- Red Flag Rules
- Health Insurance Portability and Accountability Act ("HIPAA")
- Family Educational Rights and Privacy Act ("FERPA")
- State Laws Regarding Breach Notification
- Computer Fraud and Abuse Act ("CFAA")

Gramm-Leach-Bliley Act ("GLBA") Updated Slide

- 15 U.S.C. §§ 6801 to 6809
- Applies to "financial institutions," as defined in 12 U.S.C. § 1843(k), which will include universities and colleges
- Enforced by various Federal regulators, State insurance authorities, and Federal Trade Commission
- Provides a floor regarding protection, not a ceiling
- Protects "nonpublic personal information"
- Privacy Rule prohibits disclosure, unless consumer receives sufficient notice and opt-out opportunity
- Institution in compliance with FERPA will be deemed to be in compliance with Privacy Rule of GLBA

GLBA, continued Updated Slide

- GLBA also imposes Safeguards Rule
- Institution must create a written security plan to protect such information, and must (i) designate employee to coordinate program; (ii) identify reasonably foreseeable internal and external risks; (iii) oversee and contractually bind service providers; and (iv) periodically evaluate and adjust program, depending upon circumstances and its effectiveness
- Compliance with FERPA does not mean compliance with Safeguards Rule; FERPA has no such binding requirements

Red Flag Rules – Updated Slide

- "Creditors" with "covered accounts" must comply with the Red Flag Rules in full as of ~~May 1~~ August 1, 2009 (see details on next slide)
  - "Creditor" is generally any entity that regularly extends, renews or continues credit
  - "Covered accounts" include accounts designed to permit multiple payments or transactions; thus, credit card accounts, accounts for patients, and even business credit accounts may be covered
  - "Red flag" constitutes a pattern, practice, or specific activity which suggests the risk of identity theft by someone with whom the institution is putatively dealing
- Much confusion about applicability, particularly in the healthcare sector (a reason for delay)

Red Flag Rules – Updated Slide

- On April 30, the FTC announced it would defer enforcement until August 1, 2009.
  - See FTC news release: http://www.ftc.gov/opa/2009/04/redflagsrule.shtm
  - See FTC statement: http://www.ftc.gov/os/2009/04/P095406redflagsextendedenforcement.pdf

Red Flag Rules

Identity Theft Prevention Program

- In part, RFRs require development and implementation of a written and functional identity theft prevention program ("Program")
- No "one size fits all" approach mandated by FTC
  - Program customized according to the size, nature, operational complexities and other specific characteristics of each organization
- Program must be designed to "detect, prevent, and mitigate identity theft" in connection with the covered accounts

Red Flag Rules

Identity Theft Prevention Program (cont'd)

- After an assessment of current practices and policies, each organization must create a Program that provides:
  - Policies and procedures for identifying, detecting and responding to identified red flags
    - The Program must be an evolving document, open to modifications or updates based on newly identified risks or other red flags;
  - Board-level approval and senior management oversight
    - including the provision of annual reports to the board assessing, inter alia, the effectiveness of the program, incident overview, and management's response to such incidents;
  - Training of staff to manage the program; and
  - Oversight of service provider arrangements,
    - including outsourcers, data or payment processors, and business associates

HIPAA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Covered Entities
  - Business Associates
  - Protected Health Information (PHI)
  - Privacy and Security Rules

HITECH Act impacts HIPAA

- Federal privacy breach notification rules for covered entities, business associates & personal health record (PHR) vendors
- "Temporary" notification requirements for PHR Vendors, PHR Servicers and other relevant third parties
- Health information exchanges (HIEs) and regional health information organizations (RHIOs) are business associates of covered entities
- Business Associates subject to specified sections of privacy and security rules, including civil and criminal penalties and sanctions for violations

HITECH Act impacts HIPAA (cont'd)

- Restrictions on Sale of PHI
- Accounting of all disclosures "made through" electronic health records (EHRs), *including* treatment, payment & healthcare operations (TPOs)
- Marketing restrictions
- Disclosures to be narrowed to limited data sets or minimum necessary
- State AGs may enforce HIPAA violations (civil)

Notification In Case of Breach

- Federal breach notification requirement on HIPAA covered entity (CE) that
  "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information"
- To notify each individual
  *"whose **unsecured protected health information** has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed"*

  due to the breach.

Notification (cont'd)

- Notification requirement also applies to Business Associates (BAs)
- BAs to provide notice to Covered Entity
- Notice to include "identification of each individual" whose PHI has been or is reasonably believed (by the BA) to have been breached

Notification (cont'd) – Updated Slide

- Unsecured PHI = PHI not secured through use of "technology and methodology"
- HHS issued "Guidance" on April 18, 2009, specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals
  - See HITECH Act Breach Notification Guidance and Request for Public Comment (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html)

Notification (cont'd) – Updated Slide

- Also on April 17, the FTC issued its proposed rulemaking and request for comments re breach notification requirements for commercial PHR vendors
  - See FTC's Breach Notification Rule (http://www.ftc.gov/os/2009/04/R911002healthbreach.pdf)
- Potential to decrease data loss
  - If data is secure, loss of portable devices (e.g., laptops or flash drives) will be less of an issue for healthcare providers

Notification (cont'd)

- Breach discovered on the first day it is known to a CE or BA
  - known to any employee, officer or other agent of such entity or associate, other than the person who committed the breach.
- All notifications must be made "without unreasonable delay"
  - no later than 60 calendar days after discovery
  - burden on notifying entity to demonstrate that
    - all required notifications were made and
    - explain any delays.

Notification (cont'd)

Notice must be:

- in writing, by first class mail, sent to the last known address of individual or next of kin
  - if individual specified preference for e-mail notification, that method shall be used
- one or mailings (as more information becomes available)

- If records of more than 500 residents of a state or jurisdiction are "reasonably believed to have been accessed, acquired or disclosed":
  - notices described above AND
  - notification to "prominent media outlets" in such state or jurisdiction

Notification (cont'd)

- Exception: if notice will "impede a criminal investigation or cause damage to national security
- Required contents
  - e.g., details of breach, type of information exposed, next steps and contact information
- "Possible imminent misuse" urgent situation:
  - may provide notice by phone or other appropriate means, in addition to first class mail notices

Notification (cont'd)

- Special circumstances notices
  - If insufficient/out-of-date information and
  - More than 10 affected people
    - "conspicuous posting for a period determined by the Secretary" either
      - on CE's homepage or
      - major print or broadcast media, including in individual's region (including toll-free phone number)
- Notice to the Secretary
  - Required in all cases where unsecured PHI has been acquired or disclosed
  - If more than 500 individuals affected, notice must be immediate
    - HHS to publicize breached entities on its Web site
  - If less than 500 individuals affected, CE may maintain a log & submit annually

Family Educational Rights and Privacy Act ("FERPA")

- 20 U.S.C. § 1232g; implemented at 34 C.F.R. § 99
- Safeguards "education records" and generally prohibits their release in absence of written consent
- "Education records" includes, with certain exceptions, records containing information directly relating to a student, maintained by an educational agency institution, or its agent
- Enforced by the U.S. Department of Education, Family Compliance Office; ultimate sanction is termination of federal assistance funds

FERPA Data Breach Provisions

- Notice of data breach is not required
- Rather, entity only must maintain a record of the fact of the unauthorized disclosure so that student/parent can become aware of disclosure during inspection of student's educational record (34 C.F.R. 99.32(a)(1))

FERPA Data Breach Provisions

- Federal Register (73 Fed. Reg. 74806, 74843-74844) sets forth only non-binding recommendations for safeguarding educational records and "personally identifiable information," and reacting to their unauthorized disclosure
- Methods to mitigate risk will depend on size and resources of institution, type of information to be protected, methods used by other institutions, and risks of breach and resulting harm
- Report to law enforcement, determine what (and whose) information was compromised, try to retrieve data, try to prevent further disclosures, determine how and why incident occurred, conduct risk assessment, and notify students

California Data Breach Law, SB 1386

- Applies to "person" and "business that conducts business in California," and to "personal information"
- Notification of known or reasonably believed acquisition by unauthorized person of personal information of California resident must be provided in "most expedient time possible, without delay"
- Notice must be provided via writing, electronic notice, or substitute notice (including media)

California Data Breach Law, continued

- Exemptions to notification requirement:
  - encrypted data
  - publically available government data
  - NO exemption for immaterial breaches
- Enforced through private right of action:
  - $3,000 per willful, intentional or reckless violation
  - $500 otherwise per violation

Massachusetts Data Protection Law: "Standards for the Protection of Personal Information of Residents of the Commonwealth"

- 201 CMR 17.00 to 17.05
- Deadline has been pushed back to 1/1/10
- Extremely comprehensive/onerous
- Applies to all entities storing "personal information" regarding Massachusetts resident
- Beyond notification: operational duties
  - identify and assess reasonably foreseeable risks, including those associated with third-parties
  - written security policy, with review and reporting

Computer Fraud and Abuse Act ("CFAA")

- 18 U.S.C. § 1030
- Primarily statute for criminal prosecution
- Applies to knowing or intentional unauthorized access of protected computers involving:
  - government information;
  - financial institution information;
  - conduct performed with intent to defraud or extort;
  - conduct which intentionally or recklessly causes $5,000+ in damage

CFAA, Continued

- However, also provides civil cause of action for compensatory damages or injunctive relief to "[a]ny person who suffers damage or loss . . . against the violator" when conduct did or could have caused:
  - loss to one or more persons during any one-year period aggregating at least $5,000 in value;
  - potential modification or impairment of the medical examination, diagnosis, treatment, or care;
  - physical injury to any person;
  - threat to public health or safety; or
  - damage to government computer system

How Data Breaches Can Impact Your Organization

- Government lawsuits
- Consumer/client and financial institution lawsuits
- Penalties can increase depending upon conduct
- Penalties can depend upon statute at issue, and who is enforcing it

How Data Breaches Can Impact Your Organization, Continued

- Expensive notification requirements
- Expensive efforts to investigate and ameliorate
- Embarrassing media exposure
- Undermine relationships with clients or consumers
- Undermine relationships with business partners
- Worst-case scenario for organization: insider job

How to Minimize Exposure from a Data Breach

- Limit information collected
  - No reason to collect SSN
  - Many organizations already use different identifiers
- Limit access to information stored
  - Most personnel do not need to have access to your online data systems
  - Can personnel download, email, or print information?
- Use encryption, access control and intrusion detection technology
- Dispose of records safely

How to Minimize Exposure from a Data Breach, Continued

- Know your staff
  - Consider background checks (repeated)
- Train your staff
- Know your vendors and their practices
  - Loss of tapes is a significant cause of a breach
  - Ensure vendors use most secure technology

How to Minimize Exposure from a Data Breach, Continued

- What & Where is your information
- Response Team
  - IT personnel (CIO)
  - Privacy officer
  - Legal
  - PR office
- Determine your jurisdictional requirements
  - State or federal (sector) laws which may apply

How to Respond to a Data Breach

- Determine if the breach is ongoing?
- Shut down any ongoing breach immediately
- Activate your response team
- Determine scope of breach: what data, whose data, when did the breach occur, and - if possible – how
- Notify law enforcement as appropriate
- Document events

How to Respond to a Data Breach, Continued

- What laws apply?
  - If you haven't done so earlier, this will involve determining jurisdictions of affected persons/States at issue
  - Federal requirements likely applicable as well
- How will notice be provided, when, and by who?
  Timing and nature of notice driven by applicable laws
- Determine content and text of written notice
- Determine who will receive notice, beyond individuals
  - law enforcement, credit agencies, business partners, media

How to Respond to a Data Breach, Continued

- Notify more persons than perhaps required? How assess risk?
- Forensic review of systems
- Internal investigation if appropriate
- What else?
  - Toll-free information line
  - Website posting
  - Handling the media
  - Offer credit monitoring

Communication with Law Enforcement

- Some statutes require notice to government authorities
- State law examples:
  - New York: must notify State AG, consumer protection board, and office of cyber security re: timing, content, and number of notices
  - New Jersey: must notify Division of State Police prior to disclosure to the customer
- HIPAA, as now amended: must notify Secretary of Health and Human Services, if over 500 individuals affected
- Proposed S.B. 139: must notify Secret Service within 14 days if over 10,000 individuals affected, or if database includes more than one million or is owned by the government, or involves law enforcement

Communication with Law Enforcement, Continued

- Even if not statutorily required, often advisable
- Can assist with investigation and possibly locate wrongdoers and/or stolen storage devices
- Particularly important if possible insider job
- Able to represent to others, i.e., media, affected persons, and other regulators, that authorities have been contacted
- Notification to affected persons sometimes can be delayed under statutes due to investigation by law enforcement

Law Enforcement Will Not Solve Your Data Breach Problem

- Identity theft crimes are difficult to prosecute
- Experience and available resources of law enforcement agencies can vary
- Know your facts before you make representations, particularly in regards to required disclosures
- Ultimately, organization still must spearhead proper response and review of data privacy systems

Please contact us with your questions or comments. Thanks!

- Steven J. Fox, at sjfox@postschell.com
  (202) 661-6940 in Washington, D.C.
- Peter D. Hardy, at phardy@postschell.com
  (215) 587-1001 in Philadelphia, Pennsylvania
- Robert Brandfass, at BrandfassR@vwuh.com
  (304) 598-4287 in Morgantown, West Virginia
  (Mr. Brandfass is General Counsel for West Virginia University Hospitals)