# Shakespeare On Cyberliability

Beth Cate
Associate University Counsel
Indiana University[1]

NACUA Annual Conference
Orlando, Florida
June 27, 2005

## I. Background

***"When sorrows come, they come not single spies, but in battalions". - Hamlet, Act IV, Scene V.***

Since February 15, 2005, when ChoicePoint, a commercial data broker, announced that it had sold the personal information (including credit reports and Social Security numbers) of at least 145,000 people to members of a crime ring posing as qualified customers, the newspapers have been replete with stories of unauthorized access to personal data and the corresponding risk of identity theft. How access was obtained, and what and how much data was compromised, has varied. Bank of America, Ameritrade, Time Warner, and CitiFinancial all experienced the loss or theft of unencrypted backup tapes with employee or customer data – including, for Bank of America and CitiFinancial at least, SSNs and credit card numbers – for hundreds of thousands of people, during physical transportation and storage of the tapes. The laptop of an MCI employee, containing SSNs for thousands of individuals, was stolen from her car in her home garage; the laptop was password protected but the data may not have been encrypted. In the case of Lexis Nexis, Social Security numbers and other personal data for between 278,000 and 310,000 people were improperly accessed electronically through the use of stolen passwords. In the most recently reported case, someone hacked into the computer system of CardSystem Solutions, a payment processor for several major credit card companies, and may have accessed information from up to 40 million credit and debit card accounts.

Universities are not immune to such incidents. The Privacy Rights Clearinghouse reports eighteen (18) data security breaches at universities, generally involving hacking or stolen or missing laptops, just since the ChoicePoint incident was reported.[2] Based on an informal poll of the affected schools, thus far no claims or litigation have resulted from these incidents. Nevertheless, universities need to consider the potential liability involved with security breaches.

---

[1]The views, musings, suppositions, and wild speculations expressed in this outline and during the accompanying presentation are those of the author. They do not necessarily reflect, and should not be blamed on, Indiana University or any IU office or official.

[2] http://www.privacyrights.org/ar/ChronDataBreaches.htm (current as of June 23, 2005). See also Tom Zeller Jr., "Some Colleges Falling Short in Data Security," *The New York Times*, April 4, 2005 (citing statistics from the California Office of Privacy Protection that colleges and universities accounted for 28 percent of all security breaches in the state since 2003 and more than any other group including financial institutions).

Universities grow more "wired" by the day, and have dramatically increase their reliance on electronic creation, transmission, and storage of data. University networks frequently have a decentralized and open structure. All of this heightens the potential for, and risks associated with, security breaches. Add to this the "human factor," that many if not most people using computers on campus are not "techies" and may have little intuition toward good security practices, such as using strong passwords, not sharing passwords, logging off or locking workstations, keeping sensitive data only on secure servers, avoiding spyware and harmful email attachments, and spotting phishing attacks and email scams from Nigeria seeking financial account data.[3]

When a breach occurs, universities and the individuals whose data is compromised may not know or learn whether personal data was targeted, stolen, or misused. The goal behind hacking or hardware theft may instead be to obtain the hardware itself, available server space, or a launch pad for attacks on other computer systems and networks. Regardless of whether data is ultimately misused, however, security breaches create risks of legal liability, reputational harm, and increased compliance costs. Assessing risk is difficult, because no single set of laws or standards governs the privacy and security of electronic data in university computer systems; a patchwork of federal and state statutes and state common law applies, and the common law may look to a variety of ever-changing standards and "best practices" to judge whether an institution's conduct was reasonable and lawful. Moreover, the fact that universities conduct so many electronic operations involving out of state residents – distance learning activities; web-based recruiting, admissions, financial aid, housing and other transactions; storage of personal data on alumni – creates the risk of multiple state and even international laws being asserted with respect to university information practices.

The challenge for universities, in this rapidly changing legal and technical environment, is to determine – and, as discussed below, to help define – what is expected of them regarding data privacy and security and how they will meet those expectations.

So, with apologies to Shakespeare, who never used a laptop but whose timeless words seem to capture the spirit of these issues, this outline provides an overview of some key laws and legal issues affecting electronic data privacy and security on campus, and offers some observations with respect to minimizing the risk of liability from breaches of data privacy or security—recognizing, of course, that ***"I am not bound to please thee with my answers!" – The Merchant of Venice, Act IV, Scene I***

## II. Federal Statutory Requirements for Electronic Data Privacy and Security

***"This is the short and the long of it." -- Merry Wives of Windsor, Act II, Scene II***

Several federal statutes impose obligations on universities to protect the privacy and security of electronic data and records. Three of the most significant – the Family Educational

[3] Re: succumbing to Nigerian email scams, see Wm. Shakespeare, *A Midsummer Night's Dream*, Act III, Scene II ("Lord, what fools these mortals be!").

Rights and Privacy Act (FERPA); the Health Insurance Portability and Accountability Act (HIPAA); and the Financial Services Modernization Act of 1999, more popularly known as the Gramm-Leach-Bliley Act (GLB) – are summarized below.[4] With some exceptions, these statutes avoid prescribing specific technologies or security measures, and instead either focus on the results that institutions must achieve – e.g., not permitting unauthorized disclosure of data, authenticating electronic communications – or set a general standard of reasonableness in securing personal data.

## A. Family Educational Rights and Privacy Act (FERPA)

### 1. FERPA obligations and security breaches

The most familiar of the data privacy and security statutes affecting higher education is the federal Family Educational Rights and Privacy Act (FERPA).[5] FERPA deals with student "education records," defined to mean (with a few exceptions) records containing information directly related to a student, that are maintained by a school or its agent. "Education records" is broadly defined and includes electronic records. FERPA prohibits schools from disclosing education records, or personally identifiable information in those records other than certain basic "directory information," without the student's prior written consent unless an exception applies. Disclosure means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." (emphasis added) Depending on how much intent the word "permit" is read to imply, exposing student education records to unauthorized access through inadequate security measures arguably may constitute a disclosure in violation of FERPA.

Other FERPA obligations may be affected by security and system integrity breaches. Security breaches that result in loss or alteration of student records can implicate the right of students to access and petition to correct their records. Similarly, FERPA requires schools to track disclosures of education records to third parties, as well as students who opt-out of directory information disclosures, and systems security breaches may impair a school's ability to perform these functions.

There is no private right of action to enforce FERPA[6], and statutory remedies are imposed only when a school has a "policy or practice" that violates FERPA. Inadequate computer security or known systems vulnerabilities that continue uncorrected, however, may constitute a "policy or

[4] This outline focuses on the laws that may give rise to institutional liability for failing to secure data against unauthorized access. Other state and federal laws such as the USA PATRIOT Act, the Electronic Communications Privacy Act, and state FOIA statutes, may apply to institutions' intentional disclosure of electronic data, e.g., in response to law enforcement demands or public records requests. The application of state FOIA laws to electronic information, particularly personal email and logs of internet browsing, may raise thorny conceptual, cost, and constituent relations issues. However, since "brevity is the soul of wit," -- *Hamlet*, Act II, Scene II, this outline will not attempt to review these laws and their potential impact on university operations. Discussion of these issues may be found in Kenneth D. Salomon et al., "IT Security for Higher Education: A Legal Perspective," March 20, 2003, prepared for the EDUCAUSE/Internet 2 Computer and Network Security Task Force.

[5] 20 USC § 1232g (2004); FERPA regulations are found at 34 CFR Part 99.

[6] *Gonzaga University et al. v. Doe*, 000 U.S. 01-679 (Sup. Ct. 2002).

practice" of permitting unauthorized access to student education records or violating a school's other FERPA obligations described above.

Enforcement of FERPA rests exclusively with the Department of Education's Office of Family Compliance Policy (OFCP) Students alleging improper disclosure of their records or other violations of FERPA may file a complaint with OFCP, which investigates to determine if sufficient evidence exists to conclude that a violation has occurred. If so, OFCP works with the school to achieve voluntary compliance, generally indicating steps that must be taken to comply and a time frame. In the event of noncompliance, the Department of Education may withhold or terminate eligibility for federal funds, and may also seek an injunction.[7]

### 2. Sharing electronic records with school officials and agents

A major exception under FERPA to the need for prior written consent to disclosure of student records, is that access to such records is granted to school officials with a "legitimate educational interest," i.e. who need access to the records to perform their legitimate institutional functions. In a world of databases and database access, this means that faculty and staff who have access privileges to a database must limit their use of the data therein to what is permitted by FERPA; namely, accessing only those student education records they need to perform their authorized functions, and using them only for that purpose. OFCP has emphasized the need for compliance training and strong institutional policies against misuse of authorized access to computerized databases with student education records, as a primary means of ensuring FERPA compliance:

> "Indeed, given that it is virtually impossible to use physical or technological safeguards to prevent authorized users from using their access to education records for unauthorized purposes, it is important that an educational agency or institution establish and enforce policies and procedures, including appropriate training, to help ensure that school officials do not in fact misuse education records for their own purposes."[8]

In a February 2004 interview with the Office of General Counsel of Catholic University, Leroy Rooker, Director of OFCP, also emphasized the need to track access in order to detect and address problems:

> OGC: I have heard you mention that schools that have computerized student information systems such as PeopleSoft or Banner have an obligation to track which school officials might be accessing a particular student record if the access granted by the system is broader than just to those school officials with a legitimate educational interest. For example, if the school system gives a professor access to the records of all students in a particular department, rather than just records of students who are the professor's advisees, then the school, (presumably via its software) must be able to track any inappropriate

[7] 99 CFR §99.67(a); *United States v. Miami Univ.*, 294 F.3d 797 (6th Cir. 2002) (USDOJ and DOE have standing to sue for injunctive relief to stop release of student disciplinary records; injunction granted).

[8] Letter to Strayer University, March 11, 2005, available at http://www.ed.gov/policy/gen/guid/fpco/ferpa/library/strayer031105.html.

access. In other words, the "honor system" as a defense would not fly with the Family Policy Compliance Office if there if an investigation. Am I understanding you accurately on this issue?

LR: …. If FPCO gets a complaint that someone accessed records inappropriately, and the school does not have a system that allows the school to know who accesses records, then the school has a policy or practice of permitting access to education records without knowing whether the school official has a legitimate educational interest in those records. The system has got to be one that permits the institution to know who are accessing records.[9]

Schools may treat third party service providers under contract to perform functions on the school's behalf, as school officials with a "legitimate educational interest" in accessing student records, including electronic records, provided the school includes reference to the types of third parties that may qualify in its annual notice of student rights under FERPA. Schools may then share student education records with the third party service providers, without obtaining prior written consent. Otherwise, consent is required for disclosure to third parties. With some exceptions, schools must obligate third party recipients to use the data only for its intended purpose and prohibit redisclosure without student consent. If OFCP determines a third party has improperly redisclosed student records, the school may not allow that third party further access to such records for at least five years.[10] Thus far FERPA does not expressly obligate schools to review a third party service provider's data privacy and security systems; whether OFCP will consider there to be an implied duty to do so in the electronic context, which may be more vulnerable to unauthorized access than a third party's paper files, remains to be seen.

### 3. Electronic consent to disclosure

In 2004, OFCP amended the consent provisions of the FERPA regulations to indicate that schools could rely on an electronic record and signature as the necessary "signed and dated written consent" from students authorizing disclosure of their education records.[11] The electronic record and signature must "identify[y] and authenticate[] a particular person as the source of the electronic consent; and indicate[] such person's approval of the information contained in the electronic consent." OFCP deliberately left to schools the development of electronic mechanisms that would meet these requirements, indicating that it would issue guidance but not a specific FERPA standard on electronic consent. The comments do indicate that a school may not use a PIN or password process for electronic signatures that is visible and easily accessible to persons other than the student, as that would render the PIN or password insecure.

In terms of guidance, in addition to noting the need to comply with the GLB data security requirements (discussed below), the preamble and comments for OFCP's final rule on electronic consent indicate that the Department of Education's Federal Student Aid (FSA) Standards for Electronic Signatures in Electronic Student Loan Transactions provide a "safe harbor" for security

[9] Transcript of interview available at http://counselonline.cua.edu/interviews.cfm.
[10] 99 CFR §99.33.
[11] 99 CFR §99.30(d); see Final Regulations, 69 Fed. Reg. 21669 (Apr. 21, 2004).

measures surrounding electronic records and signatures,[12] and stated that "schools may use the set-up and security measures described in the FSA Standards, particularly Sections 3-7, as guidance for security measures in a system using electronic records and signatures under FERPA."[13] Sections 3-7 list specific tools for authenticating, attributing, and confirming the intent of electronic signatures, and set standards for printing and viewing records, protecting them from alteration, tracking changes and updates, maintaining the integrity of stored records, and controlling and tracking access.

The preamble also references the federal E-SIGN law,[14] which generally gives electronic signatures and records concerning a "transaction" the same legal effect as written ones. The Uniform Electronic Transactions Act (UETA), which has been adopted by many states, likewise supports the enforceability of electronic records and signatures in "transactions."[15] "Transaction" is similarly defined in the two statutes, to mean "an action or set of actions relating to the conduct of business [or] commercial affairs" (E-SIGN also includes "consumer" affairs; UETA includes "governmental" affairs). These laws set standards for ensuring the accuracy, authenticity, integrity, preservation, and accessibility of electronic documents, but do not prescribe particular technological measures.

E-SIGN provides that whenever the law elsewhere requires certain information to be provided in writing, a party must consent in advance to receive it electronically, and demonstrate through her consent that she has the technology to receive, access, and print electronic information. Additionally, she may withdraw or refuse consent for electronic transactions at any time, and obtain the information in hard copy. UETA requires both parties to consent to transact electronically in all instances (although consent may be shown by conduct and context), and permits withdrawal of consent to future electronic transactions at any time. Accordingly, schools that wish to accept electronic student consent to disclosure of their records, or to conduct other transactions (admissions, housing, registration, and so on) with students electronically, such as through email and web forms, should should consult E-SIGN and any state adoption of UETA or other relevant state law.

### 4. OFCP Guidance on Student Identifiers

OFCP has provided the following guidance on the use of student identifiers in an electronic setting:

---

[12] The ESL standards are available at http://ifap.ed.gov/dpcletters/attachments/gen0106Arevised.pdf.

[13] Final Regulations on electronic consent, 69 Fed. Reg. at 21671.

[14] 15 USC §7001 et seq.

[15] See http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm for the Uniform Electronic Transactions Act as approved and recommended for enactment by the National Conference of Commissioners on Uniform State Laws in 1999. E-SIGN does not preempt an adoption of UETA as recommended by NCCUSL, but does preempt any alterations to the model law that are adopted by a state and are inconsistent with E-SIGN, as well as any other inconsistent state laws or state laws favoring specific technologies for addressing electronic signatures. 15 USC §7002.

- Neither the full nor partial SSN may be used to post grades to a course website; neither may a general university-issued student ID number. An ID number specifically issued for the posting of grades, and no other purpose, may be used.[16]
- A unique, university-issued ID may be designated and disclosed as directory information IF it cannot be used, on its own, to access non-directory personal information.[17]
- An institution that allows a student or third party to access education records by providing only publicly available information, such as a name or email address, without additional authentication of identity, may have a "policy or practice" in violation of FERPA because it could lead to the unauthorized disclosure of education records.[18]

## B. Health Insurance Portability and Accountability Act (HIPAA)[19]

The Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191, enacted by Congress in 1996, was intended to create a national standard for the protection of personally identifiable information relating to health care, in order to facilitate the development of an electronic health care infrastructure. HIPAA applies to "covered entities," which includes health care providers who transmit individually identifiable health information in electronic form in connection with certain standard transactions (generally related to billing). Many institutions of higher education contain units that are covered entities, and some institutions are covered entities in their entirety. The requirements of HIPAA apply only to those portions of an institution that constitute a "covered entity." Nevertheless, those requirements may spill over effectively to other operations within an institution, depending on the degree of centralization and uniformity of its information technologies operations and policies, and the extent to which the HIPAA requirements are seen as supplying "best practices" for data protection.

The mischievously titled "Administrative Simplification" portion of the law authorizes the Secretary of Health and Human Services to adopt standards regarding the electronic exchange of data relating to health care provision and coverage. Two major standards adopted by HHS – the Privacy Rule and the Security Rule – establish duties and prescribe measures to safeguard "protected health information" (PHI). PHI is individually identifiable health information that is created or received by a covered entity, that relates to past, present or future medical condition, health care treatment, or coverage of the individual. Significantly, student education records covered by FERPA, and medical treatment records otherwise defined within FERPA, are exempt from the scope of the Privacy Rule. As many institutions' covered entities handle more than just students, however, HIPAA continues to apply to those other operations.

### 1. The Privacy Rule

[16] May 29, 2001 letter to Hunter College of the City University of New York.
[17] Nov. 5, 2004 letter to University of Wisconsin-River Falls.
[18] Id.
[19] For extensive information on HIPAA and compliance with the Privacy and Security Rules, see http://www.hhs.gov/ocr/hipaa/.

The Privacy Rule is now in effect for all covered entities. Generally, it provides that covered entities may not use or disclose PHI unless the use or disclosure is (a) authorized in writing by the patient; (b) for the purpose of treatment or payment regarding that patient, or general health care operations (such as quality control); (c) for one of a number of "public interest and benefit" activities (e.g., reporting domestic abuse, complying with law enforcement demands, providing data for research purposes); or (d) incidental to a permitted use or disclosure. With limited exceptions, covered entities must make reasonable efforts to limit use and disclosure of PHI to the minimum necessary to accomplish the legitimate purpose.

The Privacy Rule also requires that covered entities give patients written notice of their privacy practices and the ways in which they may use and disclose PHI, and act in accordance with the content of the notices. Notice must be made available electronically on any web site the covered entity maintains for customer service or benefits information.

Several provisions of the Privacy Rule bear on a covered entity's obligation to maintain the integrity and security of electronic systems containing PHI.[20] A covered entity must:

- Have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of [PHI]," and "reasonably safeguard [PHI] from any intentional or unintentional use or disclosure that is in violation of the [Privacy Rule]." Policies and procedures must be reasonably designed to ensure compliance with the Privacy Rule, "taking into account the size of and the type of activities that relate to [PHI] undertaken by the covered entity…."
- Designate a privacy official who is responsible for developing and implementing its privacy policies and procedures
- Designate a contact person and provide a process for complaints
- Train all members of its workforce on its privacy policies and procedures (training may be tailored to the functions of each member)
- Have, apply, and document appropriate sanctions against members of its workforce who violate the Privacy Rule or its policies and procedures
- Mitigate to the extent practicable any harmful effect that is known to it of a use or disclosure of PHI, by the covered entity or its business associate, that violates the Privacy Rule or the covered entity's policies or procedures
- When using third parties to provide services or perform functions on its behalf that involve the use or disclosure of PHI, enter into a "Business Associate Agreement" that obligates Business Associate (BA) to use appropriate safeguards to prevent use or disclosure of the data, to flow those requirements down to subcontractors, and to report any violations of which it learns
- Take reasonable steps to cure a pattern of privacy violations by a BA, and if unsuccessful, terminate the agreement or report the BA to HHS

[20] It is important to note that, even though health care providers only become "covered entities" by virtue of electronic transmission of PHI, the Privacy Rule, unlike the Security Rule, applies to all PHI within a covered entity, not just data maintained electronically. Thus covered entities must ensure that paper records and oral transmissions of PHI are safeguarded as well.

- Adopt reasonable safeguards to ensure that incidental uses are truly incidental, and that the PHI shared is limited to the "minimum necessary."
- With limited exceptions, permit patients to:
    - review and obtain copies of their PHI;
    - request amendment of records they feel are inaccurate or incomplete;
    - obtain an accounting of disclosures of their PHI during the preceding 6 years, with some exceptions, by a covered entity or the covered entity's business associates;
    - request that covered entities restrict disclosure of PHI for treatment, payment, health care operations, and disclosures to various persons including family member. While the covered entity need not agree, if it does, it must comply; and
    - request an alternative means or location for communications of PHI.

The Privacy Rule requires that covered entities maintain documentation, in written or electronic form, of their policies and procedures, any communications required to be in writing, and anything else required to be documented under the Rule. Documents must be maintained for 6 years from creation or the last date they were in effect. Covered entities will need to ensure that electronic systems can accommodate records retention, patient requests for access and alterations, and notations with respect to patient requests for restrictions and alternative procedures.

### 2. Security Rule

The Security Rule became effective on April 21, 2005 for most covered entities (April 21, 2006 for small health plans). While the Privacy Rule determines what data is PHI and who may have access to it, the Security Rule focuses on ensuring that only those who are authorized actually do have access. The Security Rule is closely aligned with the Privacy Rule and essentially proceeds from the Privacy Rule's requirement of "appropriate administrative, technical, and physical safeguards" for PHI, fleshing out those safeguards through a series of standards, which in turn include a series of mandatory or "addressable" (discretionary) implementation specifications. A matrix of the standards, corresponding sections of the Rule, and implementation specifications (denoted R or A for required or addressable) is appended to the Rule. Although institutions will have put certain security measures in place to meet the requirements of the earlier-issued Privacy Rule, they will need to examine whether those are sufficient to meet the more extensive provisions of the Security Rule.

Mandatory specifications must be met, by implementing appropriate policies and procedures. Addressable specifications must be assessed to determine whether they are reasonable and appropriate safeguards for the particular institution, based on the reasonably anticipated security threats and hazards in its particular environment. If a specification is reasonable and appropriate, the institution may choose which security measures to use in order to meet it, considering its current risks, the security measures it already has in place, and the costs of implementation.

If a specification is not reasonable and appropriate for the particular institution, the institution must document the basis for that conclusion and either implement an reasonable and

appropriate measure that would accomplish the same purpose, or, if there is no reasonable or appropriate alternative, go forward without one as long as the underlying standard can still be met.

Here is an example of a Standard and corresponding Implementation Specification:

Standard: institutions must implement policies and procedures to prevent, detect, contain, and correct security violations.

Implementation specification (required): conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

How the specification is met – for example, whether an outside auditor is used, what gap analysis tools are used – is up to the institution.

The Security Rule's provisions were drafted to be technology neutral and scalable, in view of rapidly changing technology and widely differing types, sizes, and resources of covered entities. The standards and specifications continue to draw on concepts of reasonableness and appropriateness. While this gives institutions flexibility, it also creates uncertainty, as the reasonableness of a measure may be judged with hindsight in the event of a breach. In this regard, there may be some comfort in CMS's comment that "HHS recognizes that each covered entity is unique and varies in size and resources, and that there is no totally secure system."[21] CMS has issued a very readable and detailed series of guidance papers on implementing the security standards, which contain diagnostic question that give some insight into its expectations for particular security measures.[22] An overarching theme that emerges from the Rule and guidance is that ongoing, institution-specific risk assessment and management are the heart of a compliant security program.

### 3. HIPAA Enforcement

#### a. Complaints and compliance reviews

There is no private right of action by individuals to enforce HIPAA's data privacy protections.[23] Enforcement of the Privacy and Security Rules resides with HHS, which has delegated compliance with the Privacy Rule to the Office of Civil Rights (OCR) and compliance with the Security Rule to the Centers for Medicare and Medicaid Services (CMS). A person may file a complaint with the appropriate agency alleging a violation of the Privacy or Security Rule. The agency will investigate the complaint and work with the covered entity to achieve voluntary

[21] "Security 101 for Covered Entities," HIPAA Security Series, Vol. 2/Paper 1 (Nov. 2004), available at http://www.cms.hhs.gov/hipaa/hipaa2/education/.

[22] The series is available at the URL cited in footnote 21.

[23] See *Univ. of Colorado Hosp. Authority v. Denver Pub. Co.*, 340 F.Supp.2d 1142 (D.Colo. 2004); *Hubbs v. Alamao*, 360 F.Supp.2d 1073 (C.D. Cal. 2005).

compliance and corrective action.[24] The agency may also conduct compliance reviews; the covered entity is required to cooperate and provide access to records.

### b. Civil Monetary Penalties

If a violation is found and not corrected through voluntary compliance, HHS may impose civil monetary penalties of up to $100 per violation, capped at $25,000 during any calendar year for all violations of an identical requirement or prohibition. HHS recently published its Proposed Final Rule on Enforcement in April 2005, which would apply the same enforcement standards and mechanisms to violations of all the HIPAA rules, including both Privacy and Security Rules.[25]

Among other provisions, the Proposed Final Rule provides the factors HHS will consider in determining the number of violations for CMP, and states that conduct that may violate more than one Rule may only be assessed CMPs once. The Proposed Rule also lists aggravating and mitigating factors it may consider in calculating penalties. Several of these factors may be of particular significance in defending against penalties for a computer security breach, such as whether the violation was beyond the direct control of the covered entity and the entity's financial condition and any financial difficulties that hindered compliance.[26] In this regard, although a covered entity will be liable for CMPs under federal agency law for violations committed by its workforce, it will not be liable for violations committed by a Business Associate, as long as the covered entity had a proper BA agreement in place with the necessary assurances of compliance from the BA, and the covered entity did not know of a pattern or practice of violations by the BA and fail to act.

HHS may settle a proposed penalty for a reduced amount, and must not impose penalties at all if the conduct is punishable under the criminal provisions of HIPAA, or if HHS concludes that any of the following apply:

- the person liable for the penalty did not know of the violation and would not have discovered it through reasonable diligence;
- the failure to comply was due to reasonable cause and not to willful neglect;[27]
- the failure to comply is corrected within 30 days of becoming aware or reasonably should have become aware of the violation (HHS may extend this period)

A covered entity may request an administrative hearing to challenge a civil penalty. Before seeking judicial review of an ALJ decision, the entity must appeal the ALJ's decision to

---

[24] See Proposed Final Rule on HIPAA Enforcement, 70 Fed. Reg. 20223 (Apr. 18, 2005) ("there is one enforcement and compliance policy for the HIPAA rules. We are committed to promoting and encouraging voluntary compliance with the HIPAA rules through education, cooperation, and technical assistance."); 45 CFR Part 160.304, "Principles for Achieving Compliance" (Secretary will, to extent possible, seek cooperation of covered entities in obtaining compliance, and may provide technical assistance for voluntary compliance); 45 CFR Part 160.312(a)(1) (informal resolution of complaints); 70 Fed. Reg. 15329 (Mar. 25, 2005) (CMS complaint procedures).

[25] 70 Fed. Reg. 20223 (April 18, 2005).

[26] See Proposed Final Rule, 45 CFR Part 160.408(c)(2), (e)(1).

[27] Any penalty not entirely waived under this provision may be reduced if the penalty would be excessive compared to the compliance failure involved. 42 USC 1320d-5(b)(4).

HHS's Departmental Appeals Board. The Proposed Final Rule outlines the procedures for hearings and appeals. One of the more controversial aspects of the Proposed Final Rule is that it authorizes HHS to notify the public and appropriate state health agencies and medical or professional organizations of any final penalties.

Thus far, OCR has received over 13,000 complaints, and has not yet imposed any civil monetary penalties.[28]

### c. Criminal penalties

Criminal penalties of up to $250,000 in fines and 10 years imprisonment may be imposed on anyone who, knowingly and in violation of HIPAA, uses or causes to be used a unique health identifier, or obtains or discloses individually identifiable health information.[29] The Department of Justice enforces the criminal provisions of HIPAA, and in August 2004, secured its first conviction when a hospital consortium employee pled guilty to accessing patient personal data in order to open fraudulent credit accounts.[30] More recently, however, DOJ has concluded that the criminal penalties of HIPAA apply only to covered entities, and not to individuals, other than individuals who may be prosecuted under standard principles of corporate criminal liability, or for aiding and abetting or conspiring with the covered entity.[31]

## C. Financial Services Modernization Act of 1999, or Gramm Leach Bliley Act (GLB)

The Gramm Leach Bliley Act, 15 USC 6801 et seq. (GLB), was enacted in 1999 to enable banks to engage in a diverse assortment of commercial activities. This raised concerns, however, about the potential for widespread dissemination of customers' sensitive personal information, so the law included requirements that financial institutions safeguard nonpublic customer data, limit disclosures of such data, and notify customers of their information sharing practices and privacy policies.

GLB is enforced by a variety of federal agencies with respect to the particular financial institutions over which they have jurisdiction (SEC for brokers/dealers, Federal Reserve Board for member banks, etc.). The Federal Trade Commission has catch-all enforcement jurisdiction, over "any other financial institution or other person" that is not subject to the jurisdiction of another financial regulatory agency. The GLB Act broadly defines "financial institution" as any institution engaging in financial activities listed in 12 USC §1834(k) (the Bank Holding Company Act of 1956), which include lending activities. FTC regulations and incorporated Federal Reserve "Regulation Y" further describe covered financial activities, again including lending activities.[32] Under FTC regulations, institutions must engage in "significant" financial activities to be

---

[28] Robert Pear, "Ruling Limits Prosecutions of People Who Violate Law on Privacy of Medical Records," *The New York Times*, June 6, 2005, at A16.

[29] 42 USC 1320d-6.

[30] Robert Pear, supra.

[31] See Memorandum Re: Scope of Criminal Enforcement Under 42 USC §1320d-6, US Dept. of Justice Office of Legal Counsel (June 1, 2005), available at http://www.usdoj.gov/olc/hipaa_final.htm.

[32] 16 CFR §313.3(k); 12 CFR §225.28.

"financial institutions" covered by GLB. Because higher education institutions generally participate in a substantial amount of lending activity (and may engage in other covered activities as well), the FTC considers them covered financial institutions.[33]

Although the FTC has concluded that institutions complying with FERPA are exempt from having to comply with the privacy rules issued under GLB, it did not reach the same conclusion regarding the GLB customer information safeguarding rules. The safeguarding rules came into effect May 23, 2003.[34] They cover paper as well as electronic data[35] and extend to all nonpublic personal information, defined as personally identifiable financial information, which is in turn defined to cover a broad range of data.[36]

The requirements of the rule are brief. They contain both results-oriented standards and broad obligations, while leaving the specific means of implementation to the institutions. Institutions must develop, implement and maintain a written comprehensive information security program that contains administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the relevant customer data. The plan must be "reasonably designed" to achieve the security and confidentiality of customer data, to protect against anticipated threats or hazards, and to protect against unauthorized access or use that could result in substantial harm.

Institutions must designate an information security program coordinator, identify reasonably foreseeable risks, considering a number of areas (employee training, IT operations, and detecting, preventing, and responding to intrusions and system failures). Once risks are identified, safeguards must be implemented to control them, and regularly tested for effectiveness.

Institutions also must take reasonable steps to select and retain service providers who can handle customer information with appropriate safeguards, and obligate them contractually to do so. Finally, institutions must evaluate and adjust their security programs in light of the results of their own testing, any material changes to their operations, or "any other circumstances that you know or have reason to know may have a material impact on your information security program."[37]

As with the HIPAA Security Rule, the focus under GLB is on continual, fact-specific adjustment of an institution's security program to address the actual foreseeable risks in the institution's particular environment.[38]

---

[33] Identifying which university activities trigger GLB obligations can be a complicated exercise. For a chart analyzing common university activities and whether they may be covered by GLB, see http://counsel.cua.edu/glb/questions/frequent.cfm.

[34] See 67 Fed. Reg. 36484 (May 23, 2002).

[35] 16 CFR §314.2(b).

[36] 16 CFR §313.3(n)-(o).

[37] 16 CFR §314.4(e).

[38] For links to helpful GLB resources, including various schools' written security programs, see http://counsel.cua.edu/glb/resources/ and http://www.nacubo.org/x2152.xml. For guidance from the FTC on safeguards compliance, see http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

Some clues to how the FTC may enforce the GLB Safeguarding Rule may come from the Preamble to the Rule. In the Preamble, the agency indicates:

- that it will take into account measures that institutions adopt to comply with other data security regimes;
- that is has purposefully retained flexibility in enforcement and has not prescribed particular enforcement methods (which may allow it to follow a more cooperative model as with HHS and HIPAA);
- that it will work with smaller entities to help them achieve compliance;
- that it recognizes each institution must focus limited resources on addressing those risks most relevant to its operations;
- that it recognizes that institutions cannot perform unlimited evaluation of the security arrangements of third party service providers with whom they share data (although institutions will need to reasonably ensure the providers have sufficient procedures in place to detect and respond to security breaches and security problems that are well known in the IT community);
- that is consider the most relevant security considerations to be employee training; network and software design; information storage, transmission and disposal; and detecting, preventing and responding to attacks (this is such a broad description of important items, however, that it tends to encompass everything)

Further clues may come from the FTC's enforcement, generally in the for-profit arena, of Section 5 of the Federal Trade Commission Act. Section 5 of the FTC Act authorizes the FTC to prevent and respond to "unfair methods of competition" and "unfair or deceptive acts or practices" in or affecting commerce," and is not limited to financial products or services.[39] The FTC has brought several enforcement actions asserting that the failure to provide the level of data security described in a company's published data privacy policy was an "unfair or deceptive trade practice" under Section 5 of the Federal Trade Commission Act.[40] In most cases, the privacy policy at issue made fairly general claims about the level of data security. With the policies as a jurisdictional hook, the FTC focused on the systems security issues, rather than simply requiring amendment of the policy language to more accurately describe the level of data security the company provided. The Consent Orders resolving these cases required comprehensive data security programs and independent third party assessments of data security systems, conducted by a certified information technology security specialist on an annual or biannual basis. Certain security concerns the FTC emphasized in these cases included providing adequate security training for personnel with

[39] 15 USC §§ 41-48.

[40] See *In the Matter of* Guess?, Inc. and Guess.com, Inc., at http://www.ftc.gov/os/2003/06/; *In the Matter of* Microsoft Corporation, at http://www.ftc.gov/os/2002/08/; *In the Matter of* MTS, Inc. d/b/a Tower Records/Books/Video, at http://www.ftc.gov/os/caselist/0323209/0323209.htm; and *In the Matter of* Eli Lilly and Company, at http://www.ftc.gov/os/2002/05/. Although the FTC Act generally does not apply to nonprofit institutions, the FTC may enforce it against nonprofit membership organizations that essentially provide commercial services or benefits to its members. One such action was brought in part against the National Research Center for College and University Admissions ("NRCCUA"), a Missouri not-for-profit corporation and membership organization with more than 850 college and university members. The FTC alleged that NRCCUA, in collecting extensive personal information from millions of high school students and selling that information to commercial marketers, violated its stated privacy policies.

systems access; pre-testing new software applications in-house to ensure their security features work properly, before using them with sensitive data; and being aware of and addressing systems vulnerabilities that are well-known in the electronic security community.

More recently, the FTC has begun to suggest that even when an entity's privacy and security practices do not violate the terms of a published data privacy policy, the failure to provide adequate data security may itself constitute an "unfair method of competition" or "unfair act or practice affecting commerce" in violation of Section 5.[41] Enforcement activity along these lines may provide further insight into how the FTC will approach financial data security under GLB.

## III. State Laws Affecting Electronic Data Privacy and Security

***"Can one desire too much of a good thing?" – As You Like It, Act IV, Scene I.***

State law, as well as federal law, imposes certain data privacy and security obligations on universities, and are not wholly preempted by the federal data protection laws discussed above. For example, HIPAA does not preempt state laws that provide "greater privacy protection for the individual."[42] The Proposed Final HIPAA Enforcement Rule states that CMPs are not exclusive penalties when an act violates other state (or federal) law.

### A. Statutes

Institutions should examine their state statutes to determine any general data protection obligations they may have, such as a duty to implement reasonable security measures and record disposal methods to protect personal information,[43] a duty to use encryption in the electronic transmission of personal information,[44] obligations for certain categories of data such as health care records (for those not covered or preempted by HIPAA) and library patron records,[45] and a duty to obligate third parties receiving personal data from the institution, to protect the data with reasonable security measures.[46]

More such legislation is in the works, and SSNs are a major focus. Thirty-five states introduced legislation this year to provide or enhance protections for Social Security numbers by limiting their use and prohibiting their disclosure. Several bills require that any electronic transmission of an SSN be encrypted. Texas, Illinois, New Jersey, and South Carolina have

---

[41] Thomas J. Smedinghoff, "Trends in the Law of Information Security," 6th Annual Institute on Privacy Law: Data Protection – the Convergence of Privacy & Security, Vol. Two, pp. 291-92 (2005).

[42] 45 CFR Part 160.202.

[43] See, e.g., Calif. Civil Code § 1798.82(b) (requires reasonable security for personal data); Ark. Code 4-110-104 (same); Nev. Rev. Stat. 239B (state agencies including public universities may not disclose personal information on website except as required by law).

[44] E.g., Nev. Rev. Stat. 597.

[45] E.g., Oklahoma Stat. § 65-1-105.

[46] E.g., Calif. Civil Code 1798.82(c) ("A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."); Nev. Rev. Stat. 52.23.

introduced several bills expressly directed at institutions of higher education, which prohibit the use of the SSN or any consecutive four digits of it, as an identifier.[47] In general, the bills impose criminal penalties and civil fines for violations, and do not include a private right of action for damages.

A recent example of agency enforcement of a state statute involves the investigation of Kaiser Foundation Health Plan by the California Department of Managed Health Care (DMHC) under the California Code, for unauthorized disclosure of patient health information through an unsecured web site. The web site was created by Kaiser's IT staff as a testing portal; however, individually identifiable patient health information was placed on the site and was publicly viewable from 1999 to 2005, in violation of state law and the plan's privacy policies. DMHC fined Kaiser $200,000, in part based on its finding that Kaiser did not act to remove the data from the website or tell state regulators until the site had been reported to federal civil rights authorities and the media.[48]

## B. Common law

### 1. Tort Claims

***"Cry 'Havoc,' and let slip the dogs of war". – Julius Caesar, Act III, Scene I.***

Enterprising plaintiffs' attorneys are starting to file lawsuits based on data breach incidents. A recent article in the National Law Journal discussed consolidated actions filed against ChoicePoint and indicated that lawyers are starting to assess various tort theories, including negligence, invasion of privacy, slander, and defamation, as possible bases for identity theft claims against entities whose systems are compromised.[49]

#### a. Negligence-based actions

Negligence-based claims arising from a systems security breach might include negligence per se, when a federal or state statutory standard is violated; negligent training and supervision of employees[50]; when applicable, negligent selection of third party data service provider (e.g., a Business Associate who uses or discloses PHI in violation of HIPAA); and negligent infliction of emotional distress. Negligence generally will require claimants to show (a) that the institution had a reasonable duty of care to prevent the security breach at issue; (b) the institution violated that duty; (c) the claimants suffered actual loss or damage; and (d) the security breach caused that loss or damage.

---

[47] For the status of proposed state legislation, consult the National Conference of State Legislatures website at http://www.ncsl.org/programs/lis/privacy/SSN2005_Pending.htm.

[48] "Kaiser Foundation Health Plan Fined by State for Exposing Patient Data on the Web," Dept. of Managed Health Care Press Release, June 20, 2005, at http://www.dmhc.ca.gov/library/reports/news/prkfine.pdf.

[49] Tresa Baldas, "Data 'Fear Factor'," *The National Law Journal*, May 9, 2005.

[50] See *May v. Dartmouth Hitchcock Medical Center*, 2003 WL 21488697 (D.N.H. 2003) (citing availability in New Hampshire of action for negligent training and supervision of employees leading to improper disclosures of privileged health information).

### 1. Applicable Duty of Care

Although state and federal data protection statutes may not include their own private rights of action, courts may look to such statutes and enforcement action thereunder, to identify the relevant standards of care for the purpose of evaluating state tort claims arising from computer security incidents. This may particularly be the case when the statutes themselves impose requirements to act "reasonably," a common law tort concept.

In *Doe v. Community Health Plan-Kaiser Corp.*, 709 N.Y.S.2d 215 (2000), the court held that a medical corporation was liable for the disclosure of health information by a clerical employee, under a state tort theory of breach of the "implied covenant of trust and confidence that is inherent in the physician-patient relationship…." The court found that although various state statutes codifying the physician-patient privilege and obligation of confidentiality did not create a private right of action in themselves, such standards "define and impose the scope of the actionable duty of confidentiality which arises between certain health care providers, such as CHP, and their patients."[51]

Courts may draw from various other sources in developing a standard of care applicable to computer security, including: a university's own policy statements concerning the level of information privacy and security it provides; the FTC enforcement activity under the FTC Act, discussed above, or state enforcement activity under analogous state statutes; and "best practices" emerging within university and industry associations, including the Payment Card Industry Data Security Standard discussed in Section IV below.

Courts may also look to case law addressing the university's duty of care, as a landowner, to secure its physical premises and protect students and other invitees against third party criminal acts, in weighing the appropriate duty of care in the electronic arena.[52] Thus far courts evaluating claims alleging inadequate protection by the university against campus crime, have focused largely on whether the university reasonably could have foreseen the criminal act and resulting harm. Some courts have relied heavily on the presence or absence of prior similar criminal incidents in the same area, to judge foreseeability; others have found rape and other campus crime foreseeable based on a broader set of circumstances, including the fact that the school had taken some security precautions already, or the obvious vulnerability of the student population.[53]

---

[51] See also *Bigelow v. Sherlock*, 2005 WL 283359 (E.D. La. 2005), in which the federal court remanded a state negligence claim based in part on an alleged violation of HIPAA.

[52] See Nancy E. Tribbensee, "Liability for Negligent Security," EDUCAUSE Review (Sept./Oct. 2003).

[53] Compare *Agnes Scott College v. Clark*, 2005 WL 1220359 (Ct. App. Ga. 2005) (kidnapping from parking lot and subsequent rape during daytime were not foreseeable when no prior reported kidnappings, rapes, or other violent crimes occurring in that parking lot; only prior crimes were property crimes, and only other suspicious activities had been at night); *Reichman v. Campus View Village*, 2002 WL 31831398 (Ct. App. Ohio 2002) (assault on residence assistant at party not reasonably foreseeable when security had been called to break up parties only 5 times previously, none of which involved violence); *Gragg v. Wichita State Univ.*, 934 P.2d 121 (Kan. 1997) (gang-related shooting of spectator at fireworks show on university campus was not foreseeable, when only similar prior incident was almost 2 years earlier at another part of campus, no similar attacks at any of the 17 prior fireworks events, and surrounding area's crime rate was not so high as to suggest more security was needed); *Nero v. Kansas State Univ.*, 861 P.2d 768 (Kan. 1993) (question for jury as to whether sexual assault by one student against another, in co-ed dorm, was foreseeable, when student had already been arrested and charged with raping another student)); and *Murrell*

With respect to computer security breaches, assessing foreseeability is likely to take on broader dimensions in that breaches may involve software or other systems conditions that exist not only at the school at issue, but at other schools, organizations, and companies, nationwide and internationally. It is unclear at this point how comprehensively the courts will expect universities to know about, and respond proactively to, attacks and vulnerabilities involving other institutions. As noted above, the FTC's enforcement actions concerning data privacy and security policies suggest that the agency will expect an awareness of vulnerabilities that have been reported and discussed thoroughly in the internet community.

Certain other factors may heighten a school's duty concerning the level of computer security it provides: (1) the extent to which the school requires students and others use electronic communications in their daily activities, which may increase their exposure to potential security breaches; and (2) the magnitude of the predictable harm as measured by the amount, criticality, and sensitivity of the data compromised.

### 2. Damages/Causation

***"The attempt and not the deed confounds us." Macbeth, Act II, Scene II***

To maintain a negligence claim, a plaintiff will need to prove damages and causation. It is not yet clear whether courts will recognize as compensable the fear of being an identity theft victim due to a security breach that allows unauthorized access to one's data.[54] The strong concerns voiced in the media and the legislatures concerning identity theft may reinforce the view that the fear is justified. Interestingly, though, a new report on identity fraud issued by the Better Business Bureau and Javelin Strategy & Research, finds that the number of identity fraud victims has slightly decreased overall since 2003 (with the total cost of identity fraud slightly increasing), and that "[a]lthough there has been much recent public concern over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the method was known, 68.2% of information was obtained off-line versus only 11.6% obtained online. Conventional methods such as through lost or stolen wallets, misappropriation by family and friends, and theft of paper mail are among the

---

*v. Mount St. Clare College*, 2001 WL 1678766 (S.D. Iowa 2001) ("A college…is incapable of foreseeing an acquaintance rape that takes place in the private quarters of a student or tenant, unless a specific student or tenant has a past history of such crimes"), with *Stanton v. Univ. of Maine System*, 773 A.2d 1045 (Maine 2001) (sexual assault by acquaintance in a dorm room was foreseeable "evidenced in part by the security measures that the University had implemented"; foreseeability not dependent on evidence of prior criminal acts); *Mullins v. Pine Manor College*, 449 N.E.2d 331 (Sup. Jud. Ct. Mass. 1983) (basing duty on custom and practice of colleges to exercise due care to protect students against crime; also finding that foreseeability requires examination of all circumstances, not just prior similar crimes).

[54] See "Data 'Fear Factor" supra. Cf. *Schmidt v. US Dept. v. Veterans Affairs*, 222 FRD 592 (ED Wis. 2004) (pecuniary loss is needed to prove "actual damages" for recovery under federal Privacy Act; emotional distress is not "actual damages").

most common ways thieves gain access to information. Additionally, the likelihood of higher losses is greatest for crimes using traditional sources."[55]

Other damages may be minimal, with the increasing availability of fraud alerts and credit freezes, access to free credit reports, and the current $50 cap on liability for fraudulent credit card charges. Causation may be quite difficult to prove as well; ironically, the proliferation of security breaches that affect hundreds of thousands or millions of people may make it harder to pin down the breach that led to an instance of identity theft.[56] Finally, public institutions should check their state tort claims statutes to identify available defenses and damages caps.

**b. Non-negligence tort actions**

Many of the non-negligence tort theories that plaintiffs' counsel are reportedly considering arguably require an intent to harm that is lacking in the usual institutional breach scenario. Invasion of privacy encompasses four different theories: intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and publicity placing someone in a false light. The Restatement (Second) of Torts defines intrusion upon seclusion as "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns." Similarly, appropriation of a name or likeness is defined as "one who appropriates to his own use or benefit the name or likeness of another…." These theories do not square with the sort of security breaches universities have experienced during the past two years – largely hacking and loss or theft of hardware containing sensitive data. What the plaintiffs asserting such theories really would be saying is that institutions negligently or recklessly permitted someone else to commit the complained-of tort.

False light publicity and public disclosure of private facts do not require the same level of intent but also may pose difficulties for plaintiffs. False light publicity covers "one who gives publicity to a matter concerning another that places the other before the public in a false light…if…the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." A plaintiff might attempt to argue that an institution that was reckless about the level of its electronic data protection, had acted in reckless disregard of the resulting falsity of any identity theft or impersonation resulting from a security breach. This type of claim, and any similar defamation claim based on permitting or enabling identity theft, is still indirect however, and in the absence of actual identity theft or other demonstrable reputational damage, may be difficult to prove.

Public disclosure of private facts covers "one who gives publicity to a matter concerning the private life of another." Unless a court is willing to assume that when a system is compromised, personal data is necessarily accessed and distributed, this claim may run into proof problems as well. Both public disclosure and false light, moreover, like intrusion upon seclusion, require that the intrusion or matter disclosed be "highly offensive to a reasonable person." The

[55] Better Business Bureau and Javelin Strategy & Research, 2005 Identify Fraud Survey Report, pp. 3-4; the report is available at http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html.

[56] Given the data in the Better Business Bureau/Javelin report, supra, it may be difficult in a given case for a plaintiff to show that an electronic data incident, as opposed to a more traditional personal data misappropriation, caused her harm.

nature of the information compromised in a security breach, therefore, would bear on whether this standard is met.[57]

## IV. Contractual Security Obligations

***"…leave no rubs nor botches in the work" – Macbeth, Act III, Scene I***

As noted above, universities sharing protected data or records with third parties face certain statutory, and possibly common law, obligations to require the recipients to maintain the privacy and security of the data. As institutions turn more toward third party service providers to receive, maintain or use electronically sensitive institutional data, it is important to ensure that contracts with those service providers require them to:

- Keep data secure in accordance with applicable laws and best practices as they may change from time to time
- Fully defend and indemnify the institutions in the event of a security breach
- Maintain appropriate insurance coverage

Schools also might consider going beyond simply obligating the third party service providers to maintain data protection, and have their information technology personnel review and approve third party service provider security arrangements or prescribe particular security measures or standards that the service providers must meet. This could be done solely at the outset of the contract, or on an annual or other periodic basis throughout the relationship. As noted above, to some extent the GLB Safeguards appear to require reasonable evaluation of service providers. Of course, becoming more involved in reviewing and approving a third party's security arrangements, may increase the risk that an institution will be held responsible for failing to catch a problem or prevent a breach. Schools will need to weigh this risk against the legal and public relations risk of a perceived failure to conduct appropriate review or oversight of service providers. Informal discussions with schools that have experienced security breaches involving service providers, suggests that people whose data is compromised likely will consider the schools responsible for vendor shortcomings—if not legally, certainly in terms of the impact on relationship and reputation.

Universities that accept credit card payments for their services are on the receiving end, as well, of certain contractual obligations to secure data. Agreements with the merchant banks that process credit card transactions for universities generally contain data security obligations, and may provide for fines or other penalties in the event of a breach. Within the past year, Visa, Mastercard and other major credit card associations have issued a "Payment Card Industry Data Security Standard" and, at least for Visa, a "Cardholder Information Security Program" (CISP)

[57] In response to the recent incident at Kansas University whereby failing grades and financial aid information for a group of students were mistakenly emailed to the whole group instead of individual students, one such student suggested "she was considering filing a complaint. She said the mistake caused her embarrassment because it likely gave others an inaccurate picture of the type of student she was. She said she only took one class during the last semester and failed it because she was tending to her young daughter, who had developed pneumonia." Chad Lawhorn, "Kansas U Admits Big Mistake in Distributing Private Email," Lawrence Journal-World (June 17, 2005), at http://www2.ljworld.com/news/2005/jun/17/email/?city_local.

prescribing what to do in the event of a security breach. Merchant banks are beginning to flow these requirements down to universities with respect to securing data relating to credit card transactions.[58] The Data Security Standard is extremely detailed and comprehensive, prescribing specific security measures in addition to general programmatic elements. The Standard emphasizes tracking access to data and regularly testing and updating security measures. The CISP is similarly detailed and comprehensive, and requires immediate reporting of a breach, prompt investigation by a Visa-approved security assessor, ongoing updates concerning the investigation, and corrective action. Although these requirements will only apply directly to servers and networks that handle such data, and institutions may minimize their impact by limiting and closely controlling the resources used to process credit card transactions, these requirements may impact indirectly other security operations to the extent they are seen as contributing to best practices in data security, or otherwise inform the broader statutory or common law duties of care.

## V. Toward A Process-Based Standard of Reasonable Care

***"Though this be madness, yet there is method in 't."— Hamlet, Act II, Scene II***

Data security is something of an arms race, and what constitutes a reasonable set of data privacy and security practices will be a moving target. Even the FTC agrees that one hundred percent airtight security is not achievable. So how much security is required?

The laws surrounding information privacy and security share common objectives – ensuring availability, confidentiality, integrity and authenticity of electronic information and systems. In large part, they share conceptual approaches, setting broad or results-oriented objectives, and expecting institutions to achieve them through a continual process of assessment and adjustment that reflects the current size, complexity, and sensitivity of their data operations and the availability and cost of security measures. Thus a process-based standard of care appears to be emerging from data protection laws. That is,

> …rather than telling companies what specific security measures they must implement, developing law requires companies to engage in an ongoing and repetitive process that is designed to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments. In most cases, it does not require use of any specific security measures, instead leaving the decision up to the [institution].
>
> Key to the new legal standard is a requirement that security be responsive to a[n institution's] fact-specific risk assessment. In other words, merely implementing seemingly strong security measures is not sufficient. They must be responsive to the particular threats a[n institution] faces, and must address its vulnerabilities.

[58] The Data Security Standard is available at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf; the CISP is available at http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html#anchor_2.

Thomas J. Smedinghoff, "Trends in the Law of Information Security," 6th Annual Institute on Privacy Law: Data Protection – The Convergence of Privacy and Security, Practicing Law Institute, Vol. Two, p. 293 (2005).

The developing standard by which institutional data protection may be judged, then, is whether the institution has a living, fact-specific, comprehensive information security program in place with identified responsible officials and consisting of the following elements:

- Conducting periodic assessments of the risks the institution faces
- Developing and implementing security measures designed to manage and control the specific risks identified
- Overseeing third party service provider agreements
- Implementing security awareness training and education
- Monitoring and testing the program to ensure that it is effective
- Reviewing and adjusting the program in light of ongoing changes[59]

In addition to helping prevent security breaches in the first place, such a program also would help to underscore the unforeseeability of the threat, and the general responsible nature of the institution, in the event a breach does occur. A program that thoughtfully assesses a variety of available security options and tailors solutions to a school's own circumstances may also be better placed to argue against the reflexive application of any individual security standard, such as the Payment Card Industry Data Security Standard, when that standard is not appropriate.

## VI. Duty to Notify Regarding Security Breaches

***"The law hath not been dead, though it hath slept." – Measure for Measure, Act II, Scene II***

### A. State law

Two years ago, California enacted the first law in the country requiring notification of a systems breach that compromises the security or integrity of electronically maintained personal data.[60] The California law provides that state agencies, including public universities, and any other entities doing business in the state, that own or license electronic data containing personal information, must notify any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as a result of a computer security breach. If the data is maintained for a third party, the entity suffering the breach must also notify the third party.

[59] Thomas J. Smedinghoff, "Defining the Legal Standard for Information Security," 6th Annual Institute on Privacy Law: Data Protection – The Convergence of Privacy and Security, Practicing Law Institute, Vol. Two, p. 317 (2005). The author goes on to detail categories of security measures (technology access controls, employment policies and procedures, hardware and media disposal, and so on) to be considered and the factors that should play into the choice of any given measure (probability and criticality of risk, sensitivity of data at issue, technology and security state of the art, cost, and so on), noting that the emphasis on cost as a factor for consideration in HIPAA and GLB suggests that the government does not expect privacy and security "at all costs." Id. at 320-26.

[60] Calif. Civil Code §§ 1798.29, 1798.82.

The "personal information" covered by the statute is first name or initial and last name, together with one or more of the following: SSN, driver's license or California ID card number, or financial account number and password. If all such personal information was encrypted, however, notice is not required. Notice must be made "in the most expedient time possible and without unreasonable delay," subject to law enforcement requirements. Notice may be written or electronic (the latter must comply with the federal e-SIGN law). Substitute notice via an institution's website, notice to major statewide media, and email to those with an identifiable email address, is permitted when notice would go to more than 500,000 people or cost more than $250,000. An entity may use existing notice procedures it maintains as part of an information security policy, if they conform with the timing requirements of the statute.

The law gives some leeway to institutions to determine that notice is not required if it appears reasonably unlikely that personal information was "acquired." "Acquisition" is not defined in the statute, and it is not clear whether mere exposure to personal data, or the possibility that exposure occurred when a hacker entered a system, would suffice, depending on the facts of a particular breach. As a practical matter, however, it may be impossible in most cases to know whether information that could have been accessed, was in fact accessed, and given the spirit of the law, and the downside public relations risk of not giving notice, it is probably wise to err on the side of caution.

California's notice law has been widely credited with bringing recent data security breaches such as ChoicePoint to light, and has prompted many state legislatures to follow suit. Legislation has been introduced in thirty-five states and enacted in thirteen so far (Arkansas, Connecticut, Florida, Georgia, Illinois, Indiana, Maine, Minnesota, Montana, Nevada, North Dakota, Texas and Washington).[61] The wording of the state bills and statutes on notification is largely identical to that of California. All exempt incidents that involve encrypted data, suggesting the value of encrypting databases when possible. Enforcement is typically through the state attorneys general and violations are punishable by fine.

Some notable differences or additions are:

- Notice not required after reasonable internal investigation, and/or consultation with law enforcement, yields conclusion that breach is not likely to result in harm (Arkansas, Connecticut, Florida)
- Notice not required for technical breaches not reasonably likely to subject persons to risk of criminal activity (Washington)
- Substantial fines for ongoing failure to notify; daily and monthly fines prescribed, plus fines up to $500K available for failure to notify within 180 days (public institutions may be exempt from fines). (Florida)
- Breach must "materially compromise" data security, confidentiality, or integrity. (Florida, Montana, Nevada)

[61] For summaries, status, and links to state bills, consult the National Conference of State Legislatures website at http://www.ncsl.org/programs/lis/cip/priv/breach.htm. Georgia's statute pertains to "information brokers" and their agents and would not apply to educational institutions.

- Breach does not include unauthorized acquisition of portable electronic device that is password protected, if password was not disclosed (Indiana)
- Determination that breach is unlikely to result in harm must be documented in writing and maintained for 5 years; fine up to $50K for failure to document. (Florida)
- Notice to consumer credit reporting agencies required if breach affects more than a threshold number of people (Florida, Georgia, Indiana, Minnesota, Nevada, Texas)
- Private right of action established or not necessarily precluded (Maine, North Dakota, Washington)
- Exemption for entities covered by GLB and HIPAA (Minnesota, Nevada)
- Notice by telephone permitted (Montana)
- Coordination on notice with consumer credit reporting agencies (Montana)
- Broader definition of "personal information" (North Dakota)
- Institution may bring suit against person who unlawfully accessed or benefited from personal data; may also be granted restitution for costs of giving notice, following criminal conviction of hacker (Nevada)

### B. Proposed Federal Law

***"That it should come to this!" – Hamlet, Act I, Scene II***

Congress is also considering security breach notification legislation. S.751, sponsored by Sen. Diane Feinstein, would apply to institutions of higher education, and largely tracks the California law. It does differ, however, in some important ways:

- Covers security breaches involving paper as well as electronic records
- Does <u>not</u> exempt breaches involving encrypted data
- Imposes fines of up to $1,000 per individual affected, or up to $50,000 per day, for failure to notify
- Requires that notice contain description of the categories of information compromised; a toll-free number for the institution where an individual may learn what information was maintained about him/her, and the toll-free phone numbers and addresses of the major consumer credit reporting agencies
- Requires notice to consumer credit reporting agencies if institution is required to notify more than 1,000 individuals of breach
- Increases threshold cost estimates for substitute notice, to $500,000
- Does not necessarily preclude private right of action

S.751 would supersede inconsistent provisions of state law. The bill is currently in the Judiciary Committee; a hearing was held in April, at which tough questioning of industry witnesses by Sen. Feinstein and others suggested that there is strong sentiment for increased federal data protection measures.

## VII. <u>Insurance Considerations</u>

***"Therefore thou sleep'st so sound" – Julius Cæsar, Act II, Scene I***

Institutions are reviewing their insurance coverage for claims and other costs incurred with respect to data privacy and security breaches, such as the costs of providing notice of the breach, recovering or correcting lost data, and implementing improved security measures. Schools should review carefully whether their Comprehensive General Liability policies cover such risks. In informal discussions with members of the University Risk Management & Insurance Association, some schools reported that CGL carriers are revising their policies and writing express exclusions to deny coverage for electronic data privacy and security breaches. At the same time, some carriers are offering specific "network security" or "cyber risk" policies with multi-million dollar aggregate limits, that would cover all claims and costs associated with security breaches. Narrower "identity fraud" policies are also available to reimburse individuals whose data is compromised, up to several thousand dollars, for costs they incur as a result of the breach.

## VIII. Some Additional Suggestions for Minimizing Risk of Liability

***"If it be now, 'tis not to come; if it be not to come, it will be now; if it be not now, yet it will come: the readiness is all." -- Hamlet, Act V, Scene II***

- *"The first thing we do, let's kill all the [plaintiffs'] lawyers." - King Henry the Sixth, Act IV, Scene II*. Admittedly, not a practical solution….
- Minimize the usage of SSNs and other sensitive personal data as much as possible.
- Limit the storage of SSNs, credit card data, and other highly sensitive personal data to secure servers.
- Discuss with your institution's technology personnel the potential for using encryption in the storage and transmission of sensitive data whenever possible.
- Consider appropriate background checks for persons with access to sensitive personal data.
- Ensure that contracts with external service providers who will receive or maintain personal data contain appropriate indemnity and insurance protections, and require providers to comply with best practices; consider having your IT personnel review and approve proposed providers' data security arrangements.
- Promptly investigate breaches; when they reasonably appear to have exposed nonpublic personal information to unauthorized third parties, give notice as soon as reasonably possible[62] that is clear and appropriately apologetic or regretful, and that supplies useful information to protect against identity theft (e.g., links to information on obtaining free credit reports, placing fraud alerts or credit freezes, etc.). Provide hotline for calls and generally be as helpful as possible.[63]
- Most schools involved in recent security incidents appear not to have formal policies or procedures specific to computer security breaches, although many have general crisis response plans that may apply. Schools have tended to formulate security breach responses in an ad-hoc manner, although many of the same individuals or offices (IT senior officials, public relations personnel, legal counsel, risk management) tend to be

[62] *"Delays have dangerous ends". – King Henry VI Part I, Act III, Scene II.*

[63] See Andrew Jones' outline for this session for an excellent set of recommendations on giving notice of security breaches. See also "Recommended Practices of Notification of Security Breach Involving Personal Information," California Department of Consumer Affairs' Office of Privacy Protection (Oct. 10, 2003).

involved. Consider amending crisis response plans to address expressly computer security breaches), and organizing a "rapid response" team to address security incidents promptly, consistently, and comprehensively.[64]

- Consider having an outside security vendor conduct a proactive review of the institution's security systems, and follow up on appropriate recommendations.
- Just because students and personnel use computers every day does not mean they know how to keep data secure. Provide ongoing education on how to avoid major privacy and security risks (phishing, worms, spyware), via websites, electronic newsletters, and so on.[65]
- Include a statement in your institutional IT policies to the effect that no network is or can be 100% secure, and do not overstate the level of privacy or security afforded personal or other data maintained in or transmitted through institutional systems.
- Work with your IT professionals to identify "best practices" in higher education and commercial information practices (including the use of encryption when possible), and encourage them to work with their colleagues in higher education organizations to develop standards appropriate to and achievable by universities.

[64] Further guidance on incident response may be found in the US Dept. of Commerce National Institute of Standards and Technology's Computer Security Incident Handling Guide, Special Publication 800-61 (Jan. 2004), at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

[65] Much helpful information on common security issues, and computer use issues generally, is available at the Indiana University Knowledge Base, at http://kb.iu.edu/.