October 12, 2017

The Office of General Counsel

Data Breaches

Sarah McGee
Assistant General Counsel

Data Breaches Take Many Forms

- Hacking or Malware
  - Hacked by outside party or infected by malware
  - Using another's credentials without authorization
- Payment Card Fraud
  - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- Insider
  - Someone with legitimate access intentionally breaches information
- Physical Loss
  - Includes paper documents that are lost, discarded or stolen

Data Breaches Take Many Forms

- Portable Device
  - Lost, discarded or stolen laptop, PDA, smartphone, memory stick, CDs, hard drive, data tape, etc.
- Stationary Device
  - lost, inappropriately accessed, discarded or stolen computer or server
- Unintended Disclosure
  - disclosure (not involving hacking, intentional breach or physical loss – for example: sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax)
- Source: Privacy Rights Cleaning House https://privacyrights.org/data-breaches

Data is Regulated by Many Laws

- 1974 Privacy Act (address U.S. Government records - applies to federal contractors)
- 1974 Family Educational Rights and Privacy Act (FERPA) (education records)
- 1996 Health Insurance Portability and Accountability Act (HIPAA) (protected health information/records)
- 1999 Financial Modernization Act (Gramm-Leach-Bliley or GLB) (sets security standards for certain financial data)
- 2003 Fair and Accurate Credit Transactions Act (FACTA) (requires secure disposal of credit records)
- 2005 Payment Card Industry Data Security Standards (PCI-DSS) (sets security standards for credit card data)
- 2005 Minnesota Government Data Practices Act § 13.055 (defines “unauthorized acquisition of data”)
- 2007 Red Flag Regulations (identity theft issues in credit records)
- 2009 Health Information Technology for Economic and Clinical Health (HITECH) (privacy and security in electronic transmission of health records)
- 2018 EU General Data Protection Regulation (takes effect in May)

MGDPA
(The “data practices” act)

- Personnel data is private, unless one of several categories. Minn. Stat. § 13.43
- Donor gift data is private. Minn. Stat. § 13.792
- Data that are not public must only be accessible to persons whose work assignment reasonably requires access to the data. Minn. Stat. § 13.05, subd. 5
- Echoes FERPA in protecting educational data. Minn. Stat. § 13.32

FERPA

The Family Education Rights and Protection Act

- FERPA requires that, in general, colleges and universities must have written permission from students in order to release non-public, personally identifiable information from a student's "education record."
- Education records are those records that are:
  - (a) directly related to a student and
  - (b) maintained by an educational institution or a person acting for such agency or institution (20 USC 1232g(a)(4)(A))
- Most individually identifiable data about students and applicants in *any tangible* form – *wherever located* – is an "education record" and therefore private.
  - Applications, Transcripts, Exams, Grades
  - Class schedules
  - Photographs
  - Everything in ISRS
  - StarIDs and email addresses (unless directory data)
  - Metadata and log files
- Unless Directory Data or another exception applies

GLBA
Gramm-Leach-Bliley Act

- Regulates the collection, use, protection, and disclosure of non-public personal information by financial institutions. Goal is to restrict the sharing of customers' financial information by giving consumers rights.
- Financial Institutions are defined broadly, and the FTC has determined they includes colleges and universities based on the financial relationships they have with students, donors, and others.
- Furthermore, upon signing a Program Participation Agreement, institutions agreed to comply with GLBA.

GLBA cont'd

- The Safeguards Rule requires institutions to:
  - Develop, implement, and maintain a written information security program
  - Designate an employee responsible for coordinating the information security program
  - Identify and assess risks to customer information
  - Design and implement an information safeguards program
  - Select appropriate service providers that are capable of maintaining appropriate safeguards
  - Periodically evaluate and update their security program
- Audited beginning FY 18.

“Data Breach” Has Many Definitions

- Department of Ed (FSA)
- Security incident – any event that compromised the confidentiality, integrity, or availability of an information asset.
- Privacy breach – when PII is lost or stolen, or is disclosed or otherwise exposed to unauthorized people for unauthorized purposes. This includes PII in any format, and whether or not it is a suspected or confirmed loss
- Data Breach – An incident that resulted in confirmed disclosure, not just exposure, to an unauthorized party, often used interchangeably with data compromise.

“Data Breach” Has Many Definitions

- Department of Ed (PTAC)
  - A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release.
  - This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider.

“Data Breach” Has Many Definitions

- HIPAA:
- “Breach” means the acquisition, access, use, or disclosure of protected health information in … which compromises the security or privacy of the protected health information.
- “Breach” excludes:
  - (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
  - (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
  - (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

“Data Breach” Has Many Definitions

- GLBA
- Any unauthorized disclosure, misuse, alteration, destruction or other compromise of information.
- *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.
- ***Nonpublic personal information*** means:
  - **(i)** Personally identifiable financial information; and
  - **(ii)** Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

“Data Breach” Has Many Definitions

- MGPDA 13.055
- "Breach of the security of the data" means unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data. Good faith acquisition of or access to government data by an employee, contractor, or agent of a government entity for the purposes of the entity is not a breach of the security of the data, if the government data is not provided to or viewable by an unauthorized person, or accessed for a purpose not described in the procedures required by section 13.05, subdivision 5. For purposes of this paragraph, data maintained by a government entity includes data maintained by a person under a contract with the government entity that provides for the acquisition of or access to the data by an employee, contractor, or agent of the government entity.
  - "Unauthorized acquisition" means that a person has obtained, accessed, or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.
  - "Unauthorized person" means any person who accesses government data without a work assignment that reasonably requires access, or regardless of the person's work assignment, for a purpose not described in the procedures required by section 13.05, subdivision 5.

Event Detected: What Now? Who do you tell?

Suspected Breach Protocol

- Operating Instruction 5.23.1.13 Breach Notification
  - Under revision
- Campus to notify system office IT security (if suspected breach involves IT systems) or OGC
  - Or vice versa if the system office receives a report
  - Containment is top priority
- Notify OGC
  - Not every event is a breach
- SAME-DAY NOTIFICATION TO FEDERAL STUDENT AID OFFICE (in consultation with OGC)

Suspected Breach Protocol cont'd

- Depending on size and scope of the breach
  - Alert campus and system office communications
  - Draft crisis communications, if warranted
  - Notify appropriate cabinet officials on campus, chancellor, and board chairs
  - Other remediation measures (password resets, etc.)
- Notify the legislative auditor
- After the incident is contained and investigated
  - Draft official breach notification letters
  - Draft investigative report

New: Notice to Department of Education

- In July 2015, the Department of Education published Dear Colleague Letter GEN-15-18, reminding institutions of their obligation to protect student information.
- Letter requires immediate notification to the Federal Student Aid office by email "in the event of an unauthorized disclosure or an actual or suspected breach of [PII]."
- Not interpreted as limited to to financial aid data
- Immediate means the same day
- Receiving information requests from the Department of Ed for failure to self-report "Before Referral for Adverse Administrative Action"
  - $54,000 fines for failure to report
  - Continued participation in the federal student aid programs

Notification Under Minnesota Law

- Minn Stat 13.055, requires all state agencies to:
  - Notify individuals of any “breach in the security of data”
    - All private or confidential data (examples list)
    - In any form
    - If the data is or is reasonably believed to have been *acquired* by an *unauthorized person*.

Notification

- Requires timely Notice:
  - In the “most expedient time possible”
  - Without unreasonable delay
  - Consistent with the needs of law enforcement; or
  - Any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

Notification

- Specifies method of Notice:
  - Written by first class mail;
  - “Electronic notice” if
    - Consistent with 15 USC 7001; or
  - “Substitute” notice if cost of mailing would exceed 250k or the affected class exceeds 500,000, consisting of all the following:
    - E-mail;
    - Conspicuous posting on Web site; and
    - Notice to major media outlets that reach the general public.

Notification

- If Notice required
  - Timing
    - 10 days should be goal unless law enforcement concerns
  - Who should be notified
  - Content of notice
    - sample letter on Board Policy Website
  - Method of notice
    - Statute is specific
  - Credit Reporting Agencies?
    - Only if notice to more than 1,000

New in 2015: Investigative Report

- "[T]he responsible authority shall prepare a report on the facts and results of the investigation."
- If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agent of the government entity, the report must at a minimum include:
  - (1) a description of the type of data that were accessed or acquired;
  - (2) the number of individuals whose data was improperly accessed or acquired;
  - (3) if there has been final disposition of disciplinary action for purposes of section 13.43, the name of each employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under chapter 5B; and
  - (4) the final disposition of any disciplinary action taken against each employee in response.
- Breach notification letter must inform affected individuals that a report will be prepared, how the individual may obtain access to the report, and that the individual may request delivery of the report by mail or e-mail.

New: Office of Legislative Auditor

- State agencies are also subject to Minn. Stat. § 3.971, which contains an additional notification requirement to the Office of the Legislative Auditor (OLA). The circumstances that require a state agency to notify the OLA are much broader than the requirements of §13.055. Section 3.971 requires notification every time an entity has knowledge of improper access or use of not public data, regardless of how the unauthorized party intended to use the data.
- Examples of when the OLA notification is required, but § 13.055 data breach provision may not generally apply, include:
  - Accidental access of a not public database by a government employee
  - Incorrectly typing an email address and sending not public data to the wrong government employee
  - Inadvertently reading a report with not public data without an appropriate work assignment

Penalties for Unauthorized Access

- What are the penalties for unauthorized access to private or confidential data?
- Minnesota Statutes, section 13.09, provides that conduct which constitutes a knowing unauthorized acquisition of not public data is a misdemeanor and willful violations are subject to criminal penalties and are just cause for suspension without pay or dismissal.

Reduce Data Exposure

- Collect only PII that you are authorized to collect, and at the minimum level necessary
- Limit number of copies containing PII to the minimum needed
- Enforce a clean desk policy
- Use fictional personal data for presentations or training
- Protect data at the endpoints
  - USB drives, paper, laptops, smartphones, printers
- Destroy your data securely
- Do not keep records forever – follow retention schedules
- Limit access to only those with a need to know
- Practice breach *prevention*
  - Analyze breaches from other organizations
  - Learn from their mistakes
- Think before you post/send/tweet

Consider Data Breaches When Contracting with Cloud Providers

- When considering contracting or grant agreements with 3rd parties to perform services that include handling of non-public data (collection, transmission, cloud storage – especially electronic)
- Consult with OGC/AGO for appropriate security terms beginning with the RFP language
  - Responsibility ($$$) for Notification
  - Coordination of information
- OGC webinar in September 2015 dealt with FERPA contracting requirements for education records: http://www.minnstate.edu/system/ogc/webinars.html

Contact Information
Minnesota State Colleges & Universities
System Office

Sarah McGee

Assistant General Counsel

Sarah.McGee@MinnState.edu

651-201-1410

MINNESOTA STATE