Data Breach Response Checklist

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on https://studentprivacy.ed.gov.

Purpose

Many educational agencies and institutions have moved away from paper records toward electronic data systems and web-based applications to store, process, and deliver education data to internal customers and external partners. These systems have grown to encompass not only P-12 (pre-kindergarten through grade 12), but also post-secondary, and workforce data. They contain significant amounts of personally identifiable information (PII) from education records that must be appropriately protected and managed.

Educational organizations have a legal and ethical responsibility to protect the privacy and security of education data, including PII. The Family Educational Rights and Privacy Act (FERPA) protects PII from education records regardless of whether student records are paper or electronic; however, the best practices to protect the data do differ depending on the technology used to maintain the records. Data breaches of electronically-stored data are a growing concern affecting industry, non-profit organizations, civilian government, and defense organizations. Educational agencies and institutions at all levels should implement privacy and security best practices targeted to their unique concerns and data systems. Establishing and implementing a clear data breach response plan outlining organizational policies and procedures for addressing a potential breach is an essential step in protecting the privacy of student data. This document provides educational agencies and institutions with a checklist of critical breach response components and steps to assist them in building a comprehensive data breach response capability.

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals. Efficient incident handling will also help

reduce organizational liability associated with late or delayed actions and/or reporting, as required by applicable federal, State, or local statues.

NOTE: *The checklist discussed in this document is meant to be used as a general example illustrating some current industry best practices in data breach response and mitigation applicable to education community. This list is not exhaustive and organizations are encouraged to tailor the checklist to reflect their individual needs and priorities. Further, note that educational agencies and institutions are responsible for ensuring that their breach response plan addresses all applicable federal, State, and local data breach notification and other legal requirements. Therefore, we advise that you always consult with your organization's legal counsel to determine your organization's full responsibilities regarding applicable privacy laws.*

What is a Data Breach?

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 breaches can take many forms including

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporary misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.); and
- policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable).

In some cases, an organization may discover that control over PII, medical information, or other sensitive information has been lost for an unspecified period of time, but there is no evidence that data have been compromised. In such an instance, unless applicable federal, State, or local data breach notification laws would define this as constituting a breach, it would be up to the organization to determine whether to treat the incident as a full-scale breach or as inadequate security practice requiring immediate correction.

For educational agencies and institutions, breaches resulting in unauthorized access to PII are especially serious, as the leaked information can be used by criminals to make fraudulent purchases, obtain loans or establish lines of credit, and even obtain false identification documents. Children's data are particularly vulnerable—wrongdoers are often interested in using children's social security numbers (SSNs), permanent resident card (green card) serial numbers, naturalization document control numbers, and other PII to obtain credit or apply for benefits fraudulently, as parents or affected youth themselves may not be monitoring their credit histories until children are older.

Although electronic attacks by hackers and other cyber-criminals are a common cause of data breaches, other types of breaches occur regularly as well. "Insider threats," or threats coming from inside the organization, are also common and often involve employees accidentally, unknowingly, or maliciously mishandling, exposing, or losing sensitive data. All breaches can be equally dangerous regardless of the cause, as they leave PII and other sensitive data vulnerable to exploitation. Every educational agency and institution should, therefore, be prepared to detect and respond to the eventuality of a breach.

A part of the preparation for an effective breach response involves evaluating your organization's legal responsibilities to notify affected parties. Depending on the systems or data that are compromised, there may be legal requirements regarding notification of data owners and/or other stakeholders. Most states have some form of data breach notification laws. Federal laws, including, but not limited to, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and FERPA, all address the importance of protecting sensitive student information and may potentially apply in an event of a breach. These laws vary in their requirements regarding the right of the individual to be notified of any potential loss or access to their sensitive information. (See Resources section for a reference to the list of State Security Breach Notification Laws compiled by the National Conference of State Legislatures.)

While FERPA itself does not contain specific breach notification requirements, it protects the confidentiality of education records by requiring recordation of each incidence of data disclosure.

As stated in the preamble of the 2008 amendment to the FERPA regulations: "The [U.S.] Department [of Education] does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records. FERPA only requires that the agency or institution record the disclosure so that a parent or student will become aware of the disclosure during an inspection of the student's education record. … FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR 99.32(a)(1). In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft" (Family Educational Rights and Privacy, Final Rule, 73 Federal Register 74843-74844 [December 9, 2008]).

It is critical that educational agencies and institutions clearly understand which federal, State, and local breach notification laws apply to them, and maintain compliance with all the requirements on data breach response, reporting, and internal and external notification. To be able to fulfill breach notification requirements quickly and effectively in the event of a breach, each agency should design and implement a comprehensive data breach response plan. The plan should be kept up-to-date by conducting regular data threat assessments and by staying abreast of any changes in the relevant privacy laws.

Data Breach Checklist

While FERPA does not contain specific requirements relating to data breach, PTAC offers educational organizations a breach response checklist to help them prepare for security incidents and data breaches before they happen. Attacks against computer systems are often targeted at PII, and being able to detect, respond to, and recover from these incidents as quickly as possible can limit the amount of damage that such attacks can do. Having a robust data breach response plan, documented in writing, as part of an overarching incident response program provides an organization the tools and structure necessary to efficiently assess, manage, and mitigate a breach, while maintaining compliance with the privacy laws.

Each educational agency and institution is different and faces a unique blend of requirements and threats, which make a single prescription for data breach response impossible and undesirable. Instead, we encourage organizations to conduct their own risk assessment to identify potential threats to their data systems and to sensitive student information. To ensure effective and consistent incident response, we recommend building your response strategy around the following core components (for a more in-depth discussion and a list of specific elements within each component, see section 2.3, NIST special publication 800-61 Revision 2):

- **Policy**—*Each educational organization should create a data breach response policy, approved by the organization's leadership, that is germane to its environment. The purpose of the policy is to establish goals and vision for the breach response process. Policy should have a clearly defined scope (to whom it applies and under what circumstances), and it should include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy should be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.*

- **Plan**—*A data breach response plan is a high-level strategy for implementing the data breach policy. Individual elements of the plan should cover all phases of the incident response, from reporting the breach and the initial response activities to strategies for notification of affected parties, to breach response review and remediation process. The plan should identify the necessary organizational resources and required management support, such as senior management approval. It is important that the plan is highly tailored to your organization's unique context and is in alignment with your organization's overall mission and goals.*

- **Procedure**—*Procedures are derived from the breach response plan and codify specific tasks, actions, and activities that are a part of the data breach response effort. Procedures are designed to standardize behavior to ensure that response activities are handled in an efficient, documented, and repeatable way, while minimizing the introduction of errors. Breach response procedures should be periodically reviewed and tested in conjunction with other business continuity and disaster recovery procedures to test their effectiveness and identify areas for improvement.*

Response activities are typically fast-paced and stressful. Issues, questions, and decisions may all have potentially serious consequences on the response effort and the privacy of those affected by the breach. Therefore, staff and organizational leaders charged with responding to a breach need to be prepared to make potentially very serious decisions quickly. Establishing a robust response capability well in advance decreases the pressure on the responders and reduces errors as a result of having to "make it up as you go." As a best practice, consider conducting recurring tests, drills, and incident response exercises to help ensure your organization is prepared to respond to a breach swiftly and efficiently.

In addition to planning a data breach response, your organization should consider other preparatory steps as a part of a broader data management strategy, such as conducting regular risk assessments. These topics, however, are outside the scope of this document, which focuses specifically on the data breach response process. The remainder of this document is a checklist that incorporates current industry best practices in privacy and security. The list is tailored to the education community to assist educational organizations with creating a robust data breach response capability suitable for their environment. The two-part checklist provides suggestions on what actions to take and key issues to consider, both in preparation for a breach and after a breach has been detected. It is designed to be used as a framework to help structure internal data breach response activities, assign staff roles and responsibilities, and make appropriate policy decisions; it also provides general guidance on what actions to take in the event of a breach.

Before the Breach:

The items in this checklist are the essential building blocks of an effective and efficient data breach response plan. Addressing these items prior to a data breach incident will help educational agencies and institutions to efficiently and quickly detect and mitigate data breaches. The list below is not exhaustive and should only be used as a general guide, meant to be expanded and tailored to your organization's unique operational security needs.

☐ ***Establish and implement a written data breach response policy. The key steps involve***

- incorporating applicable breach notification legal requirements;
- addressing data breach response strategy, goals, and requirements;
- specifying incident handling procedures, strategy for deciding on the course of action in a given situation, and procedures for communicating with organizational leadership and outside parties/law enforcement;
- establishing employee expectations in conjunction with Human Resources (HR) policy and/or employee agreements;
- identifying the incident response team;
- conducting regular reviews of the policy to include any necessary improvements and ensure that it reflects up-to-date federal, State, and local requirements;
- identifying a team manager who will be in charge of the incident response (with at least one other person designated to assume authority in the absence of the manager); and
- assigning and establishing team roles and responsibilities, along with specifying access credentials.

☐ ***Review your information system(s) and data and identify where PII and other sensitive information resides. This can be done by***

- documenting what PII and other sensitive information is maintained by your organization, where it is stored (including backup storage and archived data), and how it is kept secure;
- conducting regular risk assessments and evaluating privacy threats for your organization, as well as any contractors, vendors, and other business partners;
- reviewing who is approved for access to PII and/or other sensitive information and checking user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity;
- reviewing separation of duties to help ensure integrity of security checks and balances;
- implementing mitigation controls designed to prevent and detect unauthorized access, theft, or misuse of PII and/or other sensitive data
- implementing security controls, such as encryption of sensitive data in motion and at rest (where feasible); and
- regularly reviewing and keeping up-to-date your data destruction policies, to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use.

☐ ***Continuously monitor for PII and other sensitive data leakage and loss. This includes***

- employing automated tools, like Intrusion Detection/Prevention Systems, next generation firewalls, and anti-virus and anti-malware tools, to monitor and alert about suspicious or anomalous activity;
- using Data Loss Prevention solutions to track the movement and use of information within your system, to detect and prevent the unintentional disclosure of PII and/or other sensitive data, for both data at rest and data in motion;
- conducting regular searches of the information system and physical storage areas to identify PII that may be outside of approved areas (e.g., scan your network for policy violations or occasionally police open areas for PII left unattended on desks);
- conducting internet searches to locate (and, whenever possible, remove) information that is already in the public domain or visible to the public; and
- periodically testing and checking privacy and information security controls (e.g., through the use of "real-life" exercises) to validate their effectiveness as part of a risk management program.

☐ ***Conduct frequent privacy and security awareness trainings as part of an on-going training and awareness program. This includes***

- providing mandatory privacy and information security training on a recurring basis to all employees, school officials, contractors, and any other staff involved in data-related activities;
- posting and communicating privacy policies to customers and users (for instance, on the agency web page or on a bulletin board at the office, through statements inserted in documents or emails, etc.); and
- clearly defining and making easily accessible processes for reporting privacy incidents and complaints (depending on the nature of the event, this may include reporting to the authorities, public, and/or individuals affected).

Responding to the Breach:

The following checklist provides best practice recommendations to help educational agencies and institutions create a robust data breach response plan. The list also makes recommendations regarding critical decision-making activities organizations commonly face during the breach response. Note that the checklist is not linear; some response activities may happen concurrently. The checklist is general in nature and should be adapted to meet security needs and legal requirements specific to your organization. Educational agencies and institutions should always seek legal counsel when planning for and responding to a data breach, to ensure compliance with all applicable federal, State, and local regulations.

☐ ***Validate the data breach***

- Do not assume that every identified incident is actually a breach of PII.
- Examine the initial information and available logs to confirm that a breach has occurred.
- If possible, identify the type of information disclosed and estimate the method of disclosure (internal/external disclosure, malicious attack, or accidental).

☐ ***Once a breach has been validated, immediately assign an incident manager to be responsible for the investigation***

- Assign a senior level manager, such as the Chief Information Security Officer or an individual at an equivalent director level position, to serve as an incident manager to coordinate multiple organizational units and the overall incident response. (Typically, the team manager is the incident manager; alternatively, the team manager assigns another individual to lead the response activities.)
- Begin breach response documentation and reporting process.
- Coordinate the flow of information and manage public message about the breach.

☐ ***Assemble incident response team***

- Include representatives from management, information technology, legal, public affairs/ media relations, risk management, finance, and audit departments (and possibly HR, for internal incidents) in the incident response team.
- Immediately determine the status of the breach (on-going, active, or post breach).
- If the breach is active or on-going, take action to prevent further data loss by securing and blocking unauthorized access to systems/data and preserve evidence for investigation.
- Document all mitigation efforts for later analysis.
- Advise staff who are informed of the breach to keep breach details in confidence until notified otherwise.

☐ ***Determine the scope and composition of the breach***

- If criminal activity is suspected, notify law enforcement and follow any applicable federal, State, or local legal requirements relating to the notification of law enforcement. (The decision to involve outside entities, including law enforcement, should generally be made in consultation with executive leadership and legal counsel.)
- Identify all affected data, machines, and devices.
- Conduct interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).
- When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination. Some best practices for the collection and handling of digital evidence can be found in the Resources section below.
- Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.

☐ ***Notify the data owners***

- Reach out to data owners as soon as possible to notify them about the breach.
- Foster a cooperative relationship between the incident response team and data owners.
- Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.

☐ ***Consider notifying FPCO and seeking technical assistance from PTAC***

- Consider notifying Family Policy Compliance Office (FPCO) about the breach. (FERPA does not require that you notify FPCO of the breach; however, the U.S. Department of Education considers it a best practice. While FPCO has the discretion under 34 CFR §99.64(b) to conduct its own investigation of a breach, it will take into consideration an effort to proactively come into compliance demonstrated by voluntarily notifying FPCO about the breach.) FPCO can assist educational agencies and institutions by
  - ✓ helping to determine the potential for harm resulting from the release of the information; and
  - ✓ assisting with coming into compliance with FERPA.
- After notifying data owners about the breach, consider seeking technical assistance from PTAC for informal help with security and breach prevention. PTAC can assist educational agencies and institutions by
  - ✓ providing real-word advice and best practices for responding to privacy and security incidents, notification, and data recovery;
  - ✓ assisting technical staff in conducting investigation and fact-finding activities; and
  - ✓ helping organizational decision-makers with developing a strategy for incident mitigation and data recovery.

☐ ***Determine whether to notify the authorities/law enforcement (situation dependent)***

- Consult your legal counsel to examine any applicable federal, State, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements.
- Seek involvement of law enforcement when there is a reason to believe that a crime has been committed or to maintain compliance with federal, State, or local legal requirements for breach notification.
- In concert with executive leadership and legal counsel, designate a single organizational representative (typically incident manager) authorized to initiate and/or communicate breach details to any party, including law enforcement.

☐ ***Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved***

- Decide in advance whether you will investigate a potential breach using in-house resources or an outside service provider.
- Seek advice from your legal counsel on the approved methods for protecting digital evidence, so that you are prepared and are able to properly preserve and document all evidence to ensure it can be used in a court of law, if necessary. This requires detailed recording and following proper collection, handling, storage, custody documentation, and destruction procedures (if applicable).
- If law enforcement is involved, collaborate with them to help ensure that in-house investigations do not interfere with law enforcement activities.
- Once investigative activities have been completed, safely store, record, and/or destroy (where appropriate) all evidence.
- Consider all alternatives to replacing or clearing compromised resources and machines, including the cost of remediation or rebuilding of the assets to an acceptable security level.

☐ ***Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification***

- Determine whether notification is warranted and when it should be made. Executive leadership at the senior technical and/or administrative level, in coordination with legal counsel, is the authority that should generally make this decision (for instance, at a postsecondary institution, Chief Information Officer or delegate, in consultation with the General Counsel's Office, may have the right to exert such authority).
- Notify affected individuals whose sensitive information, including PII, has been compromised, as required by applicable federal, State, and local laws.
- Provide notification in a straightforward and honest manner; avoid evasive or incomplete notifications.
- If the breach represents a threat to affected individuals' identity security, consider providing credit monitoring or identity theft protection services to mitigate the risk of negative consequences for those affected.

- Make every attempt to avoid news of the breach reaching the media before you notify affected individuals.
- Work closely with public affairs or media relations staff to craft the appropriate media notification (mailings, emails, phone calls, etc.).

☐ ***Collect and review any breach response documentation and analyses reports***

- Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence.
- Address and/or mitigate the cause(s) of the data breach.
- Solicit feedback from the responders and any affected entities.
- Review breach response activities and feedback from involved parties to determine response effectiveness.
- Make necessary modifications to your breach response strategy to improve the response process.
- Enhance and modify your information security and training programs, which includes developing countermeasures to mitigate and remediate pervious breaches; lessons learned must be integrated so that past breaches do not reoccur.

Additional Resources

References below provide best practice recommendations regarding data breach response process and tips on general information systems security. These resources include federal regulations, organizational web pages, and guidance documents prepared by third-party security experts. Please note that private sector resources (marked accordingly) should not be relied upon for legal guidance regarding data breach response. The U.S. Department of Education does not provide endorsement for private-sector resources; it simply refers them to readers for consideration.

- *Congressional Research Service, Federal Information Security and Data Breach Notification Laws* (2010): www.fas.org/sgp/crs/secrecy/RL34120.pdf

- *FERPA regulations amendment* (2011): www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

- *FERPA regulations amendment* (2008): www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf

- National Institute of Standards and Technology (NIST), NIST SP 800-61, *Computer Security Incident Handling Guide* (2012): nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- National Institute of Standards and Technology (NIST), FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

- U.S. Department of Education, Departmental Directive OM:6-107, *External Breach Notification Policy and Plan* (2008): www.ed.gov/policy/gen/leg/foia/acsom6107.pdf

- U.S. Department of Education, Family Policy Compliance Office (FPCO): https://studentprivacy.ed.gov

- U.S. Department of Education, Privacy Technical Assistance Center (PTAC): https://studentprivacy.ed.gov

- U.S. Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, *Second Edition* (2008): www.ncjrs.gov/pdffiles1/nij/219941.pdf

- U.S. Department of Justice, *Incident Response Procedures for Data Breaches Involving Personally Identifiable Information, Version 1.6* (2008): www.justice.gov/opcl/breach-procedures.pdf

Glossary

Data Loss Prevention solutions encompass a spectrum of software and hardware solutions, employed to protect sensitive data at rest and in motion from being stored, moved, or accessed in an unauthorized manner through the application of identification and filtering mechanisms.

Data owner is a term that can be used in many ways, depending on the context. For the purposes of this document, it is used to refer to an individual within an organization who is in direct control of the data and is responsible for authorizing access to or dissemination, integrity, and accuracy of the data.

Education records means records directly related to a student and maintained by an educational agency or institution, or by a party acting on behalf of the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Encryption is the process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key.

Incident manager is a key leadership role within an incident response process, typically filled by a senior level manager. The incident manager activates the incident response team, appropriates the necessary resources to investigate and manage the incident, and acts as a bridge between executive leadership (e.g., institution president, superintendent, provost, chancellor, principal, etc.), legal counsel, and information technology and law enforcement, when appropriate.

Incident response plan is a document, which establishes specific procedures for detecting, responding, mitigating, and recovering from incidents affecting organization's information systems.

Incident response team is a group of key people within an organization who are responsible for responding to computer security-related incidents.

Intrusion Detection/Prevention System is a software and hardware system, which automates monitoring of computer systems and networks for indications of security violations.

Personally identifiable information (PII) from education records includes information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education records was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010, NIST Special Publication 800-122, for more information.