FERPA Compliance and Student Data Security

1st Tamyla Nguyen
dept. of Business MIS
University of Washington Bothell
Seattle, Washington, USA
tamylngu@uw.edu

2nd Raine Johnson
dept. of Data Visualization and Cybersecurity
University of Washington Bothell
Seattle, Washington, USA
rainej1@uw.edu

***Abstract* — This paper explores the intersection of FERPA (Family Educational Rights and Privacy Act) compliance and student data security, highlighting its implications for information security practices in educational institutions. It discusses the focus on data protection security best practices aligned with FERPA, the interconnection with other compliance frameworks, and challenges in implementation.**

We address the alignment with industry standards, future directions in ensuring student data privacy, and the impact of evolving cybersecurity threats on educational institutions. The paper also considers the role of technological advancements and policy development in enhancing FERPA compliance, offering a comprehensive perspective on maintaining robust student data security.

Keywords — FERPA, student data security, information security practices, compliance, industry standards

I. Introduction

The Family Educational Rights and Privacy Act (FERPA) serves as a cornerstone for safeguarding student data privacy in educational institutions. Enacted in 1974, FERPA grants students and their parents specific rights regarding their education records, including the right to access, amend, and control the disclosure of personal information. This paper delves into the relationship between FERPA compliance and information security practices, emphasizing the imperative of protecting Personally Identifiable Information (PII) and ensuring data integrity. As educational institutions increasingly rely on digital platforms and cloud services, the challenges of maintaining FERPA compliance become more complex and necessitate a robust approach to cybersecurity. [1]

1.1. Why is it important?

Keeping user data safe is a crucial part of the cybersecurity framework. Schools store personal identifiable data that could be used in identity theft, making it imperative for FERPA to impose strict penalties on institutions that fail to safeguard this information. FERPA also provides best practices for those who do comply. Ensuring the protection of student data not only upholds legal requirements but also fosters trust among students, parents, and educational stakeholders.

II. Overview of FERPA

FERPA is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Key aspects of FERPA include:

- **Access to Records**: Students and parents have the right to access education records maintained by the school.
- **Amendment of Records**: Students and parents can request the amendment of records they believe to be inaccurate or misleading.
- **Control Over Disclosure**: Schools must have written permission from the parent or eligible student to release any information from a student's education record.

2.1 What are the specifics of FERPA?

While keeping student data protected, FERPA requires institutions to keep students up to date on whatever may be happening with the PII, ensuring student consent at every step of the way.

It’s also important to ensure that all employees handling student data are trained about the in and outs of

FERPA and what that might entail. This extends not only to academic institutions but also all third parties that may also be handling the student information. It's crucial to foster an environment where everyone knows their roles in protecting student data. [2]

There are many aspects to protecting student data, which is a prime target for attackers. Educational institutions must follow certain practices to protect data from cyber criminals. There are hefty fines imposed if a data breach occurs. Here's a few elements of FERPA compliance in IT:

- **Encrypt Data**: While in transit and at rest, all data must be encrypted. This ensures that data on a physical device, even if stolen, cannot be accessed, and data being transported over the internet also is protected. [6]
- **Test And Remediate Vulnerabilities**: There are always new vulnerabilities affecting infrastructure that stores data, including databases and cloud storage. It's important to identify issues with vulnerability scans to ensure the systems remain secure. Reviewing security controls, policies, and patch and security issues will ensure a proactive approach to preventing cyber-attacks. [6]
- **Monitoring And Audit Trails:** Ensure all systems are consistently monitored for potential threats. This includes outside threats, but more importantly, it also helps cover insider threats. Being able to detect attacks as soon as they happen helps mitigate and prevent damage. [2]
- **Continuous Updates, Reviews, And Protections:** Compliance standards often change, and regulatory bodies often give limited time to deploy updates and changes to a system to adhere to compliance. Always keep up to date with the latest circulating vulnerability, patches, and updates to ensure your systems are always up to date and protected. [2]

III. CASE STUDY: FERPA COMPLLAINT AGAINST CORNELL UNIVERSITY

A. 3.1 Complaint Overview

A student filed a complaint against Cornell University under the Family Educational Rights and Privacy Act (FERPA), alleging that the University disclosed her education records to an emeritus professor, Dr. Wolfgang O. Sack, without her consent.[6]

B. 3.2 Incident Details

The student failed the "Block I" exam twice and sought Dr. Sack's assistance in reviewing her exam.[6]

Dr. Sack's response indicated he was aware of her failing grade and the fact she was given a second chance to take the exam. [6]

Cornell argued that Dr. Sack had a legitimate educational interest as an emeritus professor and that the information was already a matter of public record due to the student's lawsuit against the University. [6]

C. 3.3 FERPA Violation

The Family Policy Compliance Office (FPCO) found that Cornell violated FERPA because Dr. Sack was not appropriately designated as a school official with legitimate educational interest in the University's annual notification to students. [6]

The FPCO clarified that disclosure of personally identifiable information from education records is prohibited without consent, even if the information is public elsewhere. [6]

D. 3.4 Cornell's Arguments for Reconsideration

Cornell cited a precedent where implied consent was inferred for disclosure in adversarial situations, arguing that the student took an adversarial position by suing the University and contacting Dr. Sack. [6]

The University maintained that Dr. Sack's involvement was appropriate given his emeritus status and the public nature of the information due to the lawsuit. [6]

E. 3.5 FPCO's Response

The FPCO reiterated that the University must designate emeritus professors as school officials with legitimate educational interest in their FERPA notification to students. [6]

The Office explained that implied consent for disclosure applies narrowly and typically only in direct litigation contexts, not routine requests for exam review. [6]

The FPCO confirmed the original finding of a FERPA violation and emphasized the need for written consent for disclosures not covered by an implied waiver. [6]

IV. IMPACT OF NON-COMPLIANCE

Non-compliance with the Family Educational Rights and Privacy Act (FERPA) can have severe consequences for educational institutions. The implications extend beyond legal penalties to include significant financial losses and reputational harm. Understanding these potential impacts underscores the critical importance of maintaining FERPA compliance.

Legal Ramifications:
Non-compliance with FERPA can result in various legal consequences, including:

1. **Loss of Federal Funding**: The U.S. Department of Education (DOE) has the authority to withhold federal funding from institutions that fail to comply with FERPA requirements. This can severely impact the financial stability of schools, particularly those that rely heavily on federal aid. [6]
2. **Lawsuits and Legal Actions**: Students and parents may sue educational institutions for breaches of FERPA. [6]
3. **Federal Investigations**: The DOE's Family Policy Compliance Office (FPCO) investigates complaints and can impose corrective actions on institutions found in violation. [6]

Financial Penalties:
The financial implications of FERPA non-compliance are multifaceted:

1. **Direct Financial Penalties**: While FERPA does not prescribe specific fines, the financial impact comes through the aforementioned loss of federal funding and costs associated with legal actions and settlements. [6]
2. **Compliance Costs**: Institutions found non-compliant must implement corrective measures, which can include upgrading security systems, enhancing training programs, and conducting extensive audits. These measures can be financially burdensome, especially for smaller institutions with limited budgets. [6]
3. **Insurance Premiums**: Institutions may face increased insurance premiums as a result of non-compliance. Data breaches and legal actions can lead to higher liability insurance costs, adding to the financial strain. [6]

Reputational Damage:
Perhaps the most lasting impact of FERPA non-compliance is the damage to an institution's reputation:

1. **Loss of Trust**: Parents and students expect educational institutions to protect their personal information. Data breaches or non-compliance can erode trust, leading to decreased enrollment and retention rates as students and families seek more secure alternatives.
2. **Negative Publicity**: Media coverage of FERPA violations can tarnish an institution's public image. Negative press can influence prospective students' decisions and impact partnerships with other educational organizations and businesses.
3. **Stakeholder Confidence**: Non-compliance can affect the confidence of stakeholders, including faculty, staff, and alumni. Internal distrust can result in decreased morale and productivity, further impacting the institution's operational effectiveness. [6]
4. **Competitive Disadvantage**: Institutions that are known for FERPA violations may struggle to compete with those that have strong compliance records. This competitive disadvantage can affect everything from student recruitment to faculty hiring and research opportunities. [6]

Long-Term Implications
The long-term implications of FERPA non-compliance can be profound. Institutions may find themselves in a continuous cycle of trying to repair their reputation while also implementing costly compliance measures. Proactive adherence to FERPA not only avoids these negative outcomes but also promotes a culture of trust and security, essential for the educational environment.

V. RECENT UPDATES AND DEVELOPMENTS IN FERPA

Recent updates to FERPA address the evolving landscape of student data privacy and cybersecurity:

Expanded Definitions: Inclusion of digital data from online tools and platforms as educational records. [1]

Enhanced Breach Protocols: Stricter procedures for notifying affected individuals and mitigating data breaches. [4]

Greater Student and Parent Rights: Improved mechanisms for consent and record amendments. [1]

Third-Party Compliance: Ensuring that external service providers adhere to FERPA regulations through rigorous vetting and contractual obligations. [4]

Technological Safeguards: Encouragement of advanced security measures like encryption and continuous monitoring. [4]

Training and Awareness: Ongoing education programs for personnel handling student data. [1]

These updates enhance FERPA's framework to better protect student data in the face of technological advancements and increasing cybersecurity threats

VI. CONCLUSION

This report has highlighted the essential role of FERPA in protecting student data privacy amidst the growing reliance on digital platforms and cloud services within educational institutions. FERPA's regulations, which grant students and parents the right to access, amend, and control educational records, are foundational to ensuring the confidentiality and integrity of personally identifiable information (PII).

To maintain compliance with FERPA, educational institutions must focus on:

- Ensuring access to records and controlling disclosure of information.
- Implementing comprehensive training programs for all personnel involved in handling student data.
- Adopting advanced technological safeguards like encryption and continuous monitoring.
- Ensuring third-party service providers adhere to FERPA regulations.

The case study involving Cornell University underscores the complexities of FERPA compliance, emphasizing the importance of clear definitions and protocols regarding access to student information and the necessity of explicit consent for disclosures.

Recent updates to FERPA, including enhanced definitions, strengthened breach protocols, expanded rights for students and parents, integration with other privacy laws, and a focus on third-party compliance, reflect the need to adapt to the evolving landscape of data security.

In conclusion, FERPA remains a critical framework for safeguarding student data privacy. Educational institutions must stay vigilant and proactive in their compliance efforts, continually updating security measures and fostering a culture of privacy and security to protect student data effectively in an increasingly digital world.

ACKNOWLEDGMENT

This report was made possible through the support of the Computing & Software Systems department at the University of Washington Bothell. Its purpose is to disseminate information regarding FERPA and the security protocols it mandates for educational institutions.

REFERENCES

[1] Bosin, Joshua I, et al. "U.S. Department of Education Issues New Ferpa Guidance on Student Health Records: Insights." *Holland & Knight*, www.hklaw.com/en/insights/publications/2023/04/us-department-of-education-issues-new-ferpa-guidance-on-student. Accessed 29 May 2024.

[2] "Data Security: K-12 and Higher Education." *Data Security: K-12 and Higher Education | Protecting Student Privacy*, studentprivacy.ed.gov/data-security-k-12-and-higher-education. Accessed 29 May 2024.

[3] "Family Educational Rights and Privacy Act (FERPA)." *EPIC*, epic.org/family-educational-rights-and-privacy-act-ferpa/#:~:text=The%20Family%20Educational%20Rights%20and,Ford%20on%20August%2021%2C%201974. Accessed 29 May 2024.

[4] "Ferpa Compliance Guide (Updated 2024): Upguard." *RSS*, www.upguard.com/blog/ferpa-compliance-guide. Accessed 29 May 2024.

[5] "Ferpa: What It Means and How It Works." *Student Press Law Center*, 17 Oct. 2018, splc.org/ferpa-what-it-means-and-how-it-works/#:~:text=Disclosure%20of%20the%20Education%20Record&text=In%20other%20words%2C%20if%20a,potentially%20loshttps://splc.org/ferpa-what-it-means-and-how-it-works/#:~:text=Disclosure%20of%20the%20Education%20Record&text=In%20other%20words%2C%20if%20a,potentially%20lose%20all%20federal%20funding.e%20all%20federal%20funding.

[6] Rooker, LeRoy S. “Letter from LeRoy S. Rooker to Dr. Hunter Rawlings III RE FERPA.” Received by Dr. Hunter Rawlings , Ithaca, 10 Apr. 2000, New York, NY.

[7] “What Is Ferpa Compliance? - Meaning, Laws & More: Proofpoint Us.” *Proofpoint*, 26 Jan. 2024, www.proofpoint.com/us/threat-reference/ferpa-compliance#:~:text=Compliance%20regulations%20aim%20to%20keep,that%20don’t%20safeguard%20it.