

CASE STUDY

Incident Summary

In July 2024, our client—an educational institution — experienced a data exposure incident. The study aims to:

- ✓ Analyze the incident and its impact
- ✓ Explore how student personal data (PII, PHI) can be better protected under FERPA



Pre- and Post-Breach Measures

A. Before the Breach

- Implemented a written data breach response policy
- Identified systems and locations storing sensitive data (PII, PHI)
- Monitored for data leakage risks
- Conducted regular privacy and security awareness training

B. Responding to the breach

Our incident response included:

- Identifying exposed data (PII, PHI, etc.)
- Reviewing documents via an eDiscovery platform following legal counsel protocols
- Mitigating risks across hundreds of employees under legal review



Data Security Process Followed

- 1 Reviewed and prioritized impacted data sets
- 2 Segregated 11+ populations for detailed analysis
- 3 Used a mix of tool-based and manual extraction
- 4 Performed deduplication, conflict checks, QC, QA, sampling, and pivot checks
- 5 Created notification lists per counsel guidance

Compliance Framework

We adhered to:

- 1 **FERPA** (Family Educational Rights and Privacy Act)
- 2 **PII** (Personally Identifiable Information) protocols
- 3 **PHI** (Protected Health Information) safeguards

Final Considerations

- The breach revealed gaps in security and compliance
- Stronger controls could have prevented unauthorized access and data exfiltration
- Our efforts ultimately secured potentially compromised data and raised security awareness.

Future Recommendations

Further research should:

- ✓ Analyze similar incidents across institutions
- ✓ Study additional regulatory compliance failures
- ✓ Examine cyber insurance, governance models, and cultural readiness

Conclusion

This breach review, supported by Aeren LPO, involved rapid turnaround to identify compromised data and notify affected individuals in a timely manner, per legal requirements.

