It’s no surprise that you have concerns about the privacy and security of sensitive data in the cloud. In 2019, there was more data stolen than ever before, with a total of 7.9 billion records compromised. The sheer amount of data circulating within and around educational institutions is on the rise. Without the right privacy controls, data security policies, and technology in place, your data is at risk of being breached.

School staff and administrators must protect student privacy in compliance with FERPA, HIPPA, FIPPA, and other regulations.

This level of security, privacy, and accessibility requires the implementation of new digital workflows and cloud-based infrastructures.

With Virtru, organizations can share sensitive data, such as student PII and PHI, with confidence, all while maintaining privacy and compliance.

“With Virtru, we found a solution that met our security and compliance requirements, was easy enough to ensure widespread adoption, and gave us the audit and control features we wanted.”

– Mark Dieterich, Director of Information Technology and Security, Brown University

Balancing Data Privacy with Secure Access.

Digital learning initiatives are becoming increasingly prevalent, creating even more data as students log in to devices from outside the physical classroom.

School staff and administrators must protect student privacy in compliance with FERPA, HIPPA, FIPPA, and other regulations.

This level of security, privacy, and accessibility requires the implementation of new digital workflows and cloud-based infrastructures.

Four Ways to Manage Your Data in the Cloud

Digital workflows, online portals, and other cloud-based applications bring plentiful opportunities to educational institutions, but they can also carry significant risks for student privacy and compliance with FERPA and other privacy regulations.

Look for a data protection solution that makes it easy to share securely across platforms and devices in any environment:

1. **End-to-End Encryption** to ensure cloud vendors and unauthorized parties will not be able to access sensitive data—such as student records, healthcare information, PII, and transcripts.

2. **Customer-Hosted Keys** that give you direct control of your data stored in the cloud, guarding against unauthorized access by email and cloud providers.

3. **Access Controls** to ensure sensitive data is only accessed by authorized collaborators and remains private, wherever it’s shared, administering the need to create new student portals, accounts, and passwords.

4. **Granular Audit** for visibility into who has accessed your proprietary data, when and where, making it easy to achieve compliance with state regulations and FERPA and HIPAA requirements.

At Virtru, we empower organizations to access the power of data while maintaining control, wherever it’s stored, accessed, or transmitted. We protect data from end to end, providing peace of mind.

Contact us to learn how Virtru can help secure your education data in the cloud.

virtru.com/contact-us