Clark Hill

Cyberthreats and K-12: EdTech Third Party Risk Management Checklist

June 27, 2023

Authors

Ilya Smith , John F. Howard

K-12 school districts across the country continue to be targeted by threat actors looking to steal sensitive personal information. Examples of this can be seen in the recent incidents affecting the Pearland Independent School District in Texas and the Tucson Unified School District in Arizona where learning is disrupted and tens of thousands of students, parents, and district employees' sensitive personal information, such as Social Security numbers, have been stolen. Years before K-12 school districts became a top target of ransomware gangs, protecting students' personally identifiable information (PII) was top of mind for several state legislators. Moving above and beyond the requirements of FERPA and COPPA, at least 34 state legislatures between 2014 and 2019 foreshadowed both the potential of EdTech transforming the learning experience and the introduction of new risks. State legislatures acted by introducing a host of student data protection requirements for K-12 school districts and EdTech to address these risks. In its 2022 Annual Report, the non-profit K12 Security Information Exchange (K12 SIX) found that "for the second calendar year running, at least 75 percent of all data breach incidents affecting U.S. public K-12 school districts were the result of security incidents involving school district vendors and other partners... the most significant vector of data breaches impacting education settings – in terms of numbers of individuals affected – are education tech vendors and other trusted non-profit and government partners."

Third-Party Risk Management — State Statutory Mandates

The state-by-state solutions to mitigate the data privacy and data security risk inherent in EdTech center on a critical strategy that is still effective today: third-party risk management. Indeed, a survey of the 34 state statutory requirements for EdTech in the K-12 space establishes requirements that must make their way into vendor agreements, where EdTech must agree to:

- Implement administrative, technical, and physical security controls
- Use limitations (i.e. can use only aggregate, de-identified data outside of “school purpose”)
- Return/Destroy student PII and education records
- Do not sell or rent student PII nor create profiles on students
- Training of vendor personnel with access to student education records and PII, and
- Establish notification procedures to schools and/or parents in event of unauthorized disclosure (like a data breach).

Additional EdTech Agreement Best Practices

These terms and conditions most often take the form of privacy policies, data sharing agreements (DSA), or data protection addendums (DPA). In addition to the above state-mandated terms, K-12 best practices to keep in mind when reviewing and negotiating these policies, DPAs, and DSAs include:

- Memorializing legal basis for collection and processing of PII and education records (i.e. designating vendor as a “school official” for FERPA purposes)
- Establishing ownership and control of the PII and education records as well as the derivative processed data
- Establishing vendor indemnification of the school district for data breaches and requirements for vendor cooperation and incident response information sharing
- Cybersecurity insurance requirement and designating the school as an “additionally insured”
- Work with school IT administrators to set SaaS and other EdTech features and processing activities to limit the collection of sensitive PII data (i.e. SSN, geolocation data etc.)
- Establish flow-down data protection requirements for vendor subcontractors
- Onboarding and training on school district privacy and security policies
- Utilization of vendor risk assessment questionnaires
- Due diligence review of vendor-written information security programs (“WISP”), incident response plana, business continuity and disaster recovery plans (i.e. backups, alternative operating procedures etc.), independent audit reports (e.g. SOC 2 Type 2), and remediation plans as applicable

Vendors are becoming more adept at responding to these requests and have information readily available for review. While negotiating technical terms and conditions can be daunting, leveraging statutory requirements presents both a justification and an imperative for the parties to work together in the best interest of students.

The views and opinions expressed in the article represent the views of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this article constitutes professional legal advice nor is it intended

to be a substitute for professional legal advice.

Related Practice Areas

Cybersecurity, Data Protection & Privacy