The Evolution of the Student Data Privacy and Security Paradigm

Incorporating the Effective Data Privacy and Security Practices of Other Sectors in Education

A RESOURCE FOR EDUCATION POLICYMAKERS AND PRACTITIONERS

David F. Katz, Steven Y. Winnick, Reginal J. Leichty, & Katherine E. Lipper,

EducationCounsel
In Affiliation with Nelson Mullins Riley & Scarborough LLP

Nelson Mullins
Nelson Mullins Riley & Scarborough LLP

Authors' Note
This paper was developed to provide support to education policymakers and practitioners for their critical work in addressing student data privacy and security in an increasingly digital age. It may prove particularly useful to state, district, and school chief privacy officers, chief financial officers, information technology specialists, and legal counsel.

Today's schools and educational agencies aim to use the remarkable power of new technologies to provide students with customized learning experiences, enhance the classroom experience, and improve student outcomes. Such capabilities hold tremendous promise – but also raise questions about how best to safeguard personal, sensitive information about students. With concerns about student data privacy and security a pressing issue in the nation's consciousness, this first-of-its-kind resource examines the ways that other industries approach data oversight, identifying opportunities for the education sector to leverage best and promising practices and build on existing work, rather than reinvent the wheel.

Acknowledgements
We thank our colleagues and partners at the Data Quality Campaign for their support and guidance during this paper's development, and for their facilitation of a panel of data privacy leaders to provide a review of a penultimate draft.

About EducationCounsel, LLC and Nelson Mullins
EducationCounsel is a mission-based education consulting firm that combines experience in policy, strategy, law, and advocacy to drive significant education improvements. Our team – including former U. S. Secretary of Education Richard W. Riley as senior partner – is a diverse and bipartisan group with a shared commitment to strengthen education systems, close achievement gaps, and expand access to educational opportunities. We work at the local, state, and national levels to develop and put into motion policy initiatives that close achievement gaps and lead to improved education outcomes from early childhood education through postsecondary education.

Nelson Mullins Riley & Scarborough LLP, which has more than 500 attorneys and other professionals in the District of Columbia, Florida, Georgia, Massachusetts, North Carolina, South Carolina, Tennessee, and West Virginia. The Nelson Mullins Privacy and Information Security Practice Group assists clients with the development, management, and oversight of privacy and compliance programs.

For more information, please visit our websites, www.educationcounsel.com and www.nelsonmullins.com.

May 21, 2015

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW 4

THE POLICY AND PRACTICE LANDSCAPE..... 7

BEST DATA PRIVACY AND SECURITY PRACTICES IN OTHER INDUSTRIES 9

A. FINANCIAL SERVICES SECTOR 9

B. HEALTHCARE SECTOR 11

C. DIGITAL APPLICATION SOFTWARE SECTOR 13

KEY RECOMMENDATIONS FOR EDUCATIONAL INSTITUTIONS 18

A. ESTABLISH THE INTERNAL GROUND RULES 18

Assess Your Data Collection Practices. *18*

Identify Your Security Objectives. *18*

Engage Key Education Administrators. *19*

Appoint a Data Leader with Responsibility for Privacy and Security Compliance. *19*

Conduct a Risk Assessment and Identify Security Needs. *19*

Ensure Internal Compliance. *20*

B. EFFECTIVELY MANAGE THIRD-PARTY VENDOR RELATIONSHIPS 22

Implement A Reasonable Vendor Approval and Governance Framework. *22*

Engage in a Risk Assessment Before a Selecting Third-Party Vendor. *23*

Use Qualified Counsel to Draft Contractual Assurances. *23*

Require Vendor Commitment to Compliance with the District or School's Privacy Policies. *23*

Assess Viability of Vendor's Own Internal Security Programs. *23*

Maintain the Right to Audit. *24*

Ensure Indemnification. *24*

Require Confidentiality and Data Stewardship. *24*

Establish Procedures for Breaches. *24*

C. COMMIT TO CONTINUOUS IMPROVEMENT IN DATA PRIVACY AND SECURITY EFFORTS AND TO TRANSPARENCY WITH RESPECT TO DATA PRACTICES 25

Commit to Improvements and Updates to Data Security Policies and Procedures. *25*

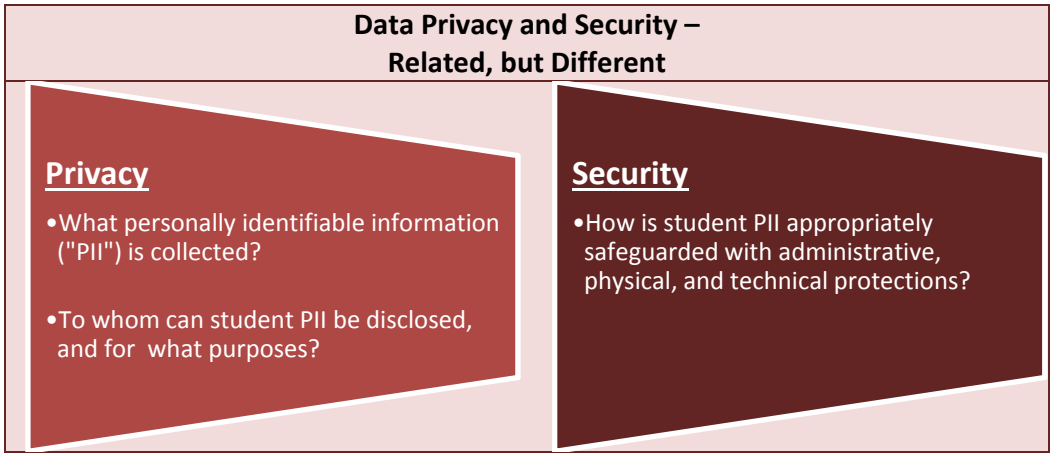
Commit to Transparency and Communication. *26*

CONCLUSION 26

INTRODUCTION AND OVERVIEW

Concern over the privacy and security of personal information has pierced the national consciousness in unprecedented ways. The ubiquitous collection, sharing, and use of personal information in the digital age have been revolutionary – and often controversial. Data privacy and security practices are far from resolved; a point evidenced by significant retail data breaches and the recent revelation of the National Security Agency's surreptitious domestic surveillance activities. Attention to privacy and security may be particularly heightened with respect to information about young people. In public education, the last two years witnessed the collapse of the business model for a prominent student data repository, the launch of a national parent organization focused on federal protections for children's personal information, and the introduction of more than 100 bills in a majority of the state legislatures focused on student data privacy and security. Concerns related to privacy have prompted expanded efforts to protect data against improper use or breaches, but they also have resulted in constraints on use of data for legitimate educational purposes.

A core principle that should inform this space is the critical need to harmonize policies and procedures to protect the privacy of student data with the need to facilitate use of that data to support and strengthen the education of students. The appropriate use of student data provides tremendous opportunities for improving schools and supporting students. Using student data, the education information technology ecosystem offers valuable resources to educators, families, students, and policymakers. New technologies can harness student data's power to tailor instruction and provide personalized education services that more effectively meet students' needs and interests. These developments reinforce why policymakers must develop and implement effective student data policies and practices that ensure privacy and security but do not unnecessarily stifle innovation and impede the development of useful education technology. Striking this balance requires careful attention to educational, technical, and legal considerations – and therefore is not an uncomplicated task.



Education policymakers should not reinvent the data privacy and security wheel. Instead, they should examine, leverage, and adapt data use standards and best privacy and security practices developed by and for other sectors of the economy. Many other industries also deal with sensitive, personal information about individuals and have grappled with issues regarding the digitalization of

that information. These sectors may be more advanced in their thinking about and implementation of appropriate safeguards, and generally have more sophisticated infrastructures, and therefore can serve as resources to the education sector. At the same time, approaches that work in one context may need to be modified to be effective in another. Through the careful evaluation of practices in these sectors, states, districts, and schools can adopt policies uniquely tailored to education and strike the appropriate balance between privacy and security and the need to encourage education technology's tremendous promise to improve education.

Examining data privacy and security practices in the financial services, healthcare, and software industries, this publication provides guidance and recommendations on the design and implementation of comprehensive student data privacy and data security policies. As data-gathering technology has advanced, many economic sectors – whether due to legal mandates, self-imposed priorities, or both – have created extensive data privacy and security infrastructures. There is significant harmony among sectors with respect to data privacy and security best practices. Policymakers and practitioners can learn from and leverage cross-sector comparisons to develop effective education data privacy and security policies in a digital age.

This publication first examines data privacy and security approaches in the financial services, healthcare, and software sectors. A landscape analysis of these three sectors is intended to help states, districts, and schools see how common issues are addressed in other fields as they consider how to best to address privacy and security in their unique contexts. The paper then makes recommendations regarding best practice standards for use in districts and schools[i] as follows:

1. **Establishing internal ground rules** by assessing your data collection practices; identifying privacy and security objectives; engaging key stakeholders and ensuring oversight of and accountability for data privacy and security compliance; conducting a risk assessment to identify security needs; implementing a security program; and ensuring compliance through background checks, training, monitoring individual and institutional activity, and accountability for all participants involved in the processing, exchange, transfer, or analysis of student data.

2. **Managing third-party vendor relationships** by putting in place a vendor approval and governance framework; executing risk assessments before selecting vendors; relying on legal counsel and a technical expert to draft agreements that include appropriate data protections and constraints on the use of data; establishing baseline standards for privacy and data security of student data; declining "contracts of adhesion" that give vendors unrestricted access to and use of data and the authority to make unilateral changes in agreements (i.e., "take it or leave it" contracts); ensuring vendor compliance with security requirements; requiring audits, indemnification, and confidentiality; and establishing responsibilities in the event of data breach.

3. **Committing to continuous improvement and transparency with respect to data practices** to ensure public understanding and support and to maintain credibility for responsible

[i] Although this guidance refers to "districts and schools", the recommendations contained herein apply equally to state educational agencies that handle student data. They apply also to institutions of higher education as well as state early learning systems.

collection and use of student data by monitoring legal requirements; leveraging information about data use and security to make improvements over time; dedicating budget dollars to maintain privacy and security controls; and promoting open communications with and educating parents, students, and educators regarding the need for secure and reasonable data collection, sharing, and use.

The paper provides significant attention to each concept embodied in these three recommendations, reflecting on how the concepts are applied in other sectors. Policymakers and practitioners should organize their data privacy and security efforts across these three broad areas, as explored below.

THE POLICY AND PRACTICE LANDSCAPE

The collection and use of personal information across many facets of our lives is nothing new. We share certain personal data whenever we sign up for a business rewards program, join the local gym, or subscribe to paid and unpaid online services. For many years, we have intuitively considered access to our personal information as a reasonable trade-off for the promises of convenience, financial savings, and other perceived incentives. But as the data collection and sharing revolution has evolved, driven particularly by the increased digitization of our personal information, the public increasingly has become aware that bad actors like hackers can easily victimize and exploit the growing public and commercial data repositories of personal information. And use of personal data has raised questions about the lengths to which corporations, governments, and private individuals will go to access information for their own interests. As the public's recognition of such risks has evolved, federal and state governments have considered appropriate regulations, and the private sector has begun increasingly to self-regulate. In essence, there is a heightened need for accountability for data use and protection in virtually ever sector of the economy, requiring all participants in the data-sharing ecosystem to consider their privacy and security practices closely.

There are certain unique considerations regarding issues of student data privacy and security. First and foremost, culturally and legally, children are valued differently from adults, worthy of special protections. Second, unlike voluntary decisions to participate in a rewards program, join a gym, or sign up for an online account (or, as discussed below, open a bank account or download a mobile application for a Smartphone), students' participation in K-12 education is mandated by law. As such, they are a captive audience for school and district data practices. The understandable sensitivities to the collection and use of student data can turn into fear and mistrust in the event of a failure of transparency and accountability by a school or district. For these very reasons, it is important that districts and schools develop and implement student data privacy and security practices that are clear and defensible and that create a sense of transparency and accountability for all parties that collect and use student data.

Student data privacy and security policies should consider at least two broad ways in which student data may be shared and used in the school setting:

1. First, certain student information is collected and maintained by the educational agency and may be used by the agency and its contractors and vendors subject to protections found in state law and the federal Family Educational Rights and Privacy Act (FERPA).
2. Second, software application and online providers, in offering services to students within the context of school programs, may collect personal student information directly from students.[ii] This arrangement is covered, to some extent, by state law and the federal Children's Online Privacy Protection Act (COPPA) and Protection of Pupil Rights Amendment (PPRA).

[ii] Student information also might be provided by a teacher who serves as a conduit between the online service provider and the student. Where the shared student information is not maintained by the school or district in the student's official student record, it is not clear that FERPA would apply to this disclosure. For example, the teacher might upload individual pieces of student work to use the services of an online tool or resource.

When crafting student data policies, both situations should be addressed and federal and state student data privacy and security laws and attendant guidance should be consulted.

Federal Privacy Laws that Apply to Students and Children *Include…*[1]	
Family Educational Rights and Privacy Act (FERPA)	The foundational federal law on the privacy of students' educational records, FERPA safeguards student privacy by limiting who may access student records, specifying for what purpose they may access those records, and detailing what rules they have to follow when accessing the data.
Children's Internet Protection Act (CIPA)	CIPA requires K–12 schools and libraries receiving federal discounts for internet access to implement internet safety polices that prevent students from accessing inappropriate and/or harmful materials and that protect against the unauthorized disclosure, use, and dissemination of minors' personal information.
Children's Online Privacy Protection Act (COPPA)	COPPA regulates how commercial entities may collect and use information collected online from children under age 13, including rules about parental consent.
Protection of Pupil Rights Amendment (PPRA)	PPRA defines the rules states and districts must follow when administering tools to students like surveys, analyses, and evaluations funded by the U.S. Department of Education. It requires parental approval to administer such tools and ensures that school districts have policies in place regarding how the data collected through these tools can be used. It also requires that plans be developed in consultation with parents regarding the collection and disclosure of personal information from students for the purpose of marketing or selling that information or providing that information to others for that purpose and requires that parents (or students of an appropriate age) be given an opportunity to opt out of such collections or disclosures.

State laws likely add other requirements with respect to student data, with a majority of state legislatures addressing student data privacy and security in new statutes. Of the 46 states with legislative sessions in 2014, alone, 36 introduced student data privacy bills (110 bills explicitly addressed the safeguarding of education data), and 20 states passed 28 student data privacy and security bills into law.

With unique considerations regarding student data in mind, an examination of the practices for data privacy and security in other sectors of the economy can be a very useful exercise. Like education, industries such as financial services, healthcare, and software need and use confidential, personal information to provide individuals (customers, patients, and users, respectively), with high-quality, personalized services. These sectors similarly are subject to laws and regulations as well as self-regulated industry standards, and as data become increasingly digitized, they face similar challenges. These sectors also may be more advanced in the implementation of certain privacy and security safeguards and have more sophisticated infrastructures. Districts and schools that wish to craft appropriate data protection policies and procedures can consider approaches taken in these fields as they design, implement, and maintain student data privacy and security controls – while recognizing unique needs and challenges in the education space. The following section examines relevant data practices in the financial services, healthcare, and software industries.

A. FINANCIAL SERVICES SECTOR

Overview

To provide their customers with quality services, financial institutions like banks, credit unions, mortgage brokers, and professional tax preparers collect some of the most personal information about their customers – names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and social security numbers – and often link this information to accounts that house personal investments. This information can make the industry a prime target for security threats.[2]

Given this landscape, the financial services industry is subject to legal rules regarding the collection and use of customer information. In addition to state laws that may govern how companies conduct business in certain jurisdictions, the federal Gramm-Leach-Bliley Act ("GLBA")[3] places data collection and disclosure requirements on financial services institutions. Companies must ensure the security and confidentiality of customer information and protect against security threats. GLBA also requires that customers receive clear notice regarding a financial services company's privacy practices and have the right to opt out of having certain information shared with certain nonaffiliated or unrelated third parties that are unconnected to the financial institution.[4] (This "opt out" right does not extend to situations where a financial institution shares information with an outside company that provides essential services like data processing or servicing of accounts.)

As one federal agency that implements GLBA, the Federal Trade Commission ("FTC") has issued the Safeguards Rule, which requires financial institutions to have certain measures in place to keep customer information secure.[5] Under the Safeguards Rule, financial companies must designate at least one employee to coordinate an information security program, evaluate the effectiveness of current safeguards and make adjustments as needed, and select service providers that maintain appropriate data safeguards. Relevant to this last requirement, the U.S. Department of Treasury, Office of the Comptroller of the Currency recently issued guidance for banks and federal savings associations on third-party relationships.[6] The guidance provides recommendations on selecting a vendor, negotiating a contract, engaging in ongoing monitoring, and reviewing the contractor's plans for key personnel changes and the timely return or destruction of the bank's data to adhere to privacy obligations.

In addition to the requirements in GLBA and federal agency regulations as well as federal guidance (and any relevant state statutes), the financial services sector has established industry standards. For example, the payment card processing industry established voluntary standards to help govern the use of customer credit card data. The Payment Card Industry Data Security Standard ("PCI-DSS") creates a framework for companies that collect and store cardholder data.[7] Requirements under PCI-DSS include building a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.[8]

Best Data Security Practices in the Financial Services Sector:
Federal Trade Commission Safeguards Rule[9]

The Federal Trade Commission is one of several federal agencies that implement the Gramm-Leach-Bliley Act. Its Safeguards Rule mandates that financial companies maintain a written information security plan that describes their programs to protect customer information. In accordance with the Rule's requirements, financial companies must comply with the following:

- Designate at least one employee to coordinate its information security program;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that maintain appropriate safeguards (with contracts that require contractors to maintain safeguards) and oversee their handling of customer information; and
- Evaluate and adjust the security program in light of relevant circumstances, including changes in the company's business or operations, or the results of security testing and monitoring.

Financial Services Data Security in Third-Party Relationships

Under GLBA, when a financial institution shares nonpublic consumer information with a third-party service provider, it must "fully disclose the providing of such information and enter into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information."[10] Several federal agencies enforce this requirement, including the Department of Treasury's Office of the Comptroller of the Currency (which regulates national banks); this office requires that contracts with third-party vendors prohibit the redisclosure or use of the information for any purpose other than the one for which the disclosure was made.[11]

Given these legal requirements, the selection of third-party vendors in the financial services industry requires a deliberate and thorough process of risk evaluation, with financial institutions conducting due diligence on each vendor to ensure its ability to conduct business in compliance with laws and regulations. (Guidance from different federal agencies addresses this work.[12]) Financial institutions conduct reference checks to reveal a vendor's history of service (including complaints and any litigation) and are guided to examine prospective vendors' business goals, service philosophies, and operational policies to ensure appropriate alignment with their own strategic goals, objectives, and risk management policies. A vendor's ability to respond to service disruptions or breaches is very important for the financial services sector.

A key component of contract negotiations with third-party vendors in the financial services industry is data security. Federal agencies enforcing GLBA recommend that written contracts give emphasis to expectations, roles, rights and responsibilities, accuracy, and legal compliance above speed and volume of transactions. They also recommend that contracts include indemnification and insurance clauses and require vendors to have an information security program and plan for mitigating known and possible threats. In accordance with federal guidance, a financial institution should engage in ongoing monitoring of its vendors, requiring proper documentation and reports. The contract

governing the parties' relationship is recommended to include periodic independent audits with results reported to senior management. At the conclusion of the contractual relationship, the vendor should return or destroy personal data to maintain privacy obligations.

B. HEALTHCARE SECTOR

Overview

From major hospital complexes to primary care physician offices, the healthcare industry needs private and, in most cases, intimately personal information about patients in order to provide high-quality services, perform critical research, and improve health outcomes. Increasingly, health information is captured digitally, for example in online health portals that provide patients with easy access to test results and medical records. Given the sensitivity and value of health information, data breaches in the healthcare sector – whether the result of purposeful thefts or the consequence of negligent oversight – are a major concern.[13]

Pursuant to federal law, healthcare providers, health plans (including employer-sponsored plans), and healthcare clearinghouses (such as billing agents) – called "covered entities" – must comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[14] HIPAA establishes national standards for safeguarding "protected health information" ("PHI"), defined to include information that could identify a person related to a past, present, or future health condition or the provision of healthcare. Under the U.S. Department of Health & Human Services' ("DHHS") HIPAA Privacy Rule,[15] a covered entity may not disclose PHI for any purpose other than treatment, payment, or healthcare operations unless the covered entity has the individual's authorization or the disclosure comes within a limited number of HIPAA exceptions. HIPPA further requires covered entities to take a number of data privacy and security steps, including designating a privacy officer and contact person, establishing privacy and disclosure policies, training and sanctioning employees, and issuing a privacy notice to patients concerning use and disclosure of PHI. (Meanwhile, the Affordable Healthcare Act incorporates HIPAA requirements while authorizing the collection of medical data on centralized databases to facilitate better coordinated care and reduce administrative overhead.[16])

In addition to federal mandates (and any similar state requirements), the healthcare industry produces resources and tools on data use and protection. These resources direct healthcare organizations to create data inventories and incident response teams as steps for protecting patient information.[17] Industry resources also examine data security with respect to third-party relationships, with directives to assess vendor access to and security of healthcare data, implementing at least annual security and privacy audits, and ensuring appropriate contractual terms with respect to data access and use.[18]

Healthcare Data Security in Third-Party Relationships

To protect patient health data, healthcare entities covered by HIPAA must ensure that vendors maintain appropriate controls. DHHS's Privacy Rule applies only to covered entities, but most healthcare providers and plans do not carry out all of their activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered entities to disclose protected health information to these "business associates" if the healthcare entities obtain satisfactory assurances that the vendors will use information only for the purposes for which it was engaged by the covered entity, will safeguard the information from

misuse, and will help the covered entity comply with some duties under the Privacy Rule. Covered entities may disclose protected health information to a vendor *only* to help the covered entity carry out its healthcare functions – not for the vendor's independent use or purposes. DHHS regulations further require that HIPAA-covered healthcare entities obtain satisfactory assurances from their vendors regarding data use (and vendors must obtain the same assurances from any subcontractors).[19]

Best Data Security Practices in the Healthcare Sector:
HIPAA Requirements for Covered Entities[20]

HIPAA requires covered entities to do the following:

- Institute a required level of security for health information, including limiting disclosures of information to the minimum required for the activity;
- Designate a privacy officer and contact person;
- Establish privacy and disclosure policies to comply with HIPAA;
- Train employees on privacy policies;
- Establish sanctions for employees who violate privacy policies;
- Establish administrative systems in relation to the health information that can respond to complaints, respond to requests for corrections of health information by a patient, accept requests not to disclose for certain purposes, and track disclosures of health information;
- Issue a privacy notice to patients concerning the use and disclosure of their protected health information; and
- Establish a process through an internal review board or a privacy board for a HIPAA review of research protocols.

In light of these legal requirements, healthcare entities routinely scrutinize vendors with access to personally identifiable health information, continuously evaluating those relationships that may pose the greatest security risk. Examination of vendors may range from conducting a comprehensive and detailed risk assessment for vendors with access to critical information to a more limited review for those with only occasional access to personal information. As it assesses vendors' data practices, a healthcare institution must determine whether the vendor has the security measures required under its contract in place. Failure by all parties to abide by the privacy and security requirements under the contract can result in violations of law and can expose both the covered entity and the vendor to substantial fines and penalties.

C. DIGITAL APPLICATION SOFTWARE SECTOR

Overview

In contrast to the financial services, healthcare, and education industries, there is no federal statute or regulation that governs data privacy issues in the software sector specifically.[21] Software is an ever-present component of our 21st-Century lives thanks to the Internet, computers, and mobile devices, and as a relatively new sector, the industry's privacy and security efforts remain in flux as new digital capabilities are realized. Thus, data privacy and security practices in the software industry are a significant issue for privacy, civil liberties, and consumer advocates; software developers and publishers; and other entities in the software ecosystem as the field aims to strike the appropriate balance between (1) instilling trust in software products and protecting individuals' sensitive information and (2) encouraging innovation and optimizing the consumer experience.

As noted above, some states are beginning to pass laws about software data-sharing activities that impact children – and the federal government also is considering whether legislation is appropriate.[22] Additionally, state and federal agencies have issued guidance on software application ("app"[iii]) data privacy and security practices, and the field itself has released voluntary standards in an effort to self-regulate. These resources relate to direct relationships between software providers and their users. In the education setting, districts and schools must consider whether and how to manage relationships between software providers and *students* – for example, whether student access to software apps will be limited, whether teachers will be entrusted to determine which applications will be used, etc. As part of this focus, districts and schools need to address what training on privacy and security is required for those entrusted to make these determinations and what standards and processes must be used. Resources related to the software application industry include specific attention to privacy and security considerations for products intended for use by children,[23] and the information in this section is intended to be helpful to policymakers in assessing such questions.

The four federal privacy laws discussed in the introduction of this resource may be implicated by the use of apps in schools. COPPA, which regulates the online collection of information from children under age 13, empowers school districts to consent to a website or app's collection, use, or disclosure of student personal information where the collection is for the use and benefit of the school and for no other commercial purpose – for example, a homework help website or a web-based testing service.[24] Under CIPA, schools participating in the federal E-rate program must establish internet safety policies that address unauthorized disclosure, use, and dissemination of personal information regarding students. FERPA applies when the relationship between a software provider and student contributes data to the student's education record, and PPRA may be relevant when the software or app is used to administer a survey, analysis, or evaluation of students and is federally funded, or if personal information is to be collected from students for a marketing or sales purpose.

In light of significant activity during recent state legislative sessions, state laws increasingly may regulate the role software providers play in school settings. In September 2014, for example,

[iii] An "app" is a self-contained program or piece of software designed for a particular purpose. Typically used via a Smartphone or tablet, an app is a standalone software program that enables the user to access a particular tool or resource (e.g., Facebook, ESPN, interactive games, etc.) without using an Internet browser.

California's governor signed into law a suite of bills aimed at enhancing privacy and security protections for student data. California law now prohibits online K-12 service providers from selling or using student data for marketing purposes; requires service providers to implement and maintain reasonable security procedures and practices; and requires that school districts create privacy standards for their contracts with third-parties that operate online sites and applications or provide schools with web-based services, including services to collect and analyze student data.[25] California law also prevents vendors from using, sharing, disclosing, or compiling personal information about students for purposes other than those specified in contracts with districts. Responsibilities thus are placed not only on K-12 schools and districts but also on the software industry itself. (In early 2015, President Obama called for federal legislation focused on student data privacy, touting California's recent law as an example.[26])

Beyond this legal regime, federal and state government actors have issued guidelines for the software sector, specifically targeting app developers and platforms. For example:

- The Federal Trade Commission released guidance for app platforms and developers. With respect to developers, the FTC encouraged making privacy policies accessible to users and implementing just-in-time notices that require affirmative express consent from users before collecting and sharing sensitive information.[27]

- The National Telecommunications and Information Administration ("NTIA") at the U.S. Department of Commerce released a voluntary "Short Form Notice Code of Conduct" for mobile apps.[28] Mobile app developers that commit to this code must include in their short-form notices (1) the types of data they collect (specifically, biometric; browser history; phone/text log; contacts; financial information; health, medical, or therapy information; location; and user files); (2) the means for accessing the company's long-form privacy policy; (3) data shared with third parties; and (4) the app provider's identity. NTIA also provides suggestions regarding the design of the short-form notice, noting elements including screen size, form factors, text and font size, and timing of notice.

- In January 2013, California's Attorney General (after securing the commitment of six major mobile application market companies to a set of consumer privacy principles[29]) produced a set of privacy recommendations. Among the suggestions, app platforms are encouraged to make each app's privacy policy easily accessible, provide users with tools to report apps for noncompliance, and educate users on mobile privacy.[30] And app developers are instructed to analyze the personal data they collect to assess whether the collection is necessary; how data will be used, stored, accessed, and shared (including with third parties); and whether data on children is implicated. App developers further should establish privacy practices that have certain elements including minimization of data collection, limited retention of data, and security safeguards regarding limited access, encryption, and compliance with the Payment Card Industry Data Security Standard (discussed above, in the financial services sector) where applicable.

In addition to government guidance, the software industry itself is promoting data stewardship commitments. In 2014, the Software & Information Industry Association, a trade association for the software and digital content industry, identified the following five best practices for software providers of school services:[31]

1. Personally identifiable information about students should be collected, used, and shared only for an educational and related purpose.
2. Software providers should disclose in their contracts and privacy policies what types of student data are collected and the purpose of the use or sharing of these data.
3. Software providers collect, use, and share student information only in accordance with permission obtained via authorization from educational institutions or the consent of parents or students.
4. Software providers maintain security policies and procedures to protect student data.
5. Software providers have reasonable policies and procedures for a data breach.

The Association for Competitive Technology, an organization representing software companies in the mobile app community, released the App Privacy Icons as part of its App Trust Project.[32] The Privacy Icons help consumers easily consider whether an app includes in-app advertisements, social media integration (linking to Facebook or Instagram, for example), location tracking (identifying where the user is located via the GPS in the Smartphone or tablet), hyperlinks to websites, and in-app purchase functionality.

Best Data Security Practices in the Software Sector:
GSMA's *Privacy Design Guidelines for Mobile Application Development*[33]

The GSM Association (GSMA), an association of mobile operators and companies, encourages app developers to embed privacy in a proactive manner and implement privacy guidelines, which include:

1. ***Transparency, choice, and control*:** Identify and minimize data collected. Disclose your identity to users. Let users exercise rights (e.g., view data collected, correct and update data). Require user consent for secondary and non-obvious uses of data. Require consent when material changes are made in the way data are collected and used.

2. ***Data retention and security:*** Actively authenticate users. Use technical measures and business processes to keep data secure. Implement authentication mechanisms. Set retention and deletion periods, destroying user data as soon as possible.

3. ***Education***: Educate users about privacy implications and settings.

4. ***Social networking/social media:*** Be careful about mapping registration information to public profiles. Ensure default settings are privacy-protective. Take measures to protect children from endangering themselves (defaults).

5. ***Mobile advertising***: Inform users about advertising features embedded in mobile apps. Require user consent to targeted ads that result from tracking users' online activities.

6. ***Location:*** Inform users if their location will be used (via GPS functionality of their Smartphone or tablet) and give them choice to deactivate.

7. ***Children and adolescents:*** Tailor apps to appropriate age ranges. Set privacy-protective default settings. Verify age when possible and appropriate.

8. ***Accountability and enforcement:*** Assign a company representative responsibility for privacy. Provider users with tools to report problems.

Finally, a number of badges and seals have been developed to identify software that adheres to certain data privacy and security practices. For example, MOMs With Apps, which is supported by the Association for Competitive Technology, provides a logo that signals that an app designed for children has provided special attention to online privacy.[34] The kidSAFE Seal Program, developed by a consulting firm focused on privacy, identifies children-friendly websites and technologies including gaming websites, mobile apps, and social networks.[35]

Privacy Tools for Parents Navigating the Software App Sector

Association for Competitive Technology's App Privacy Icons:

MOMS with Apps Checklist:

1. **Privacy policies and disclosure:**
   - ✓ **Do you have a privacy policy?**
   - ✓ **Does it cover how your app works, so parents know what you do and don't do with data?**
   - ✓ **Is your privacy policy clear and concise, and written in language parents can understand?**
   - ✓ **Are highlights of the privacy policy disclosed in your app store description?**
   - ✓ **Is your privacy policy displayed prominently on your website, from the app store, and within the app?**
   - ✓ **Does your policy include contact information?**
2. **Family friendly app design:**
   - ✓ **Does your app contain links that can lead a child outside the app? If so, have you integrated them thoughtfully, with respect for little hands?**
3. **COPPA compliant:**
   - ✓ **Are you familiar with the COPPA FAQs so you can evaluate your apps against the regulations?**
   - ✓ **Have you read the privacy policies of any third-party services or plug-ins included in your app and are you confident they are treating your customer's data in a COPPA compliant fashion?**

kidSAFE Seal Program seals:

- Safety measures for chat and community features (if applicable)
- Rules and educational information about online safety
- Procedures for handling safety issues and complaints
- Parental controls over child's account
- Age-appropriate content, advertising, and marketing

- Neutral age questions
- Parental notice and consent procedures (when applicable)
- Parental access to child's personal information (when applicable)
- Data integrity and security procedures
- COPPA-compliant privacy policy
- COPPA oversight and enforcement by the kidSAFE® Seal Program

Software User Data Security in Third-Party Relationships

As referenced above, many apps share user information with third parties, including advertisers, data analytics companies, government entities, operation systems and platforms, and social networks. The guidelines and resources discussed above, whether produced by government entities or the software sector itself, note that app developers must specifically assess data privacy and security with respect to third-party relationships.

A central component of this assessment is the focus on appropriate notification of privacy policies to software users. With respect to government entities, the California Office of the Attorney General recommends that app developers provide users with links to third-parties' privacy policies; the FTC presses app developers to disclose to users what information third parties collect and how they use that data; and the NTIA requires that short-form privacy notices include information about sharing of user-specific data with third parties. The NTIA Code of Conduct qualifies that an app developer does not need a third-party disclosure if the developer and third party have a contract that (1) explicitly limits the third-party data uses solely to providing a service to or on behalf of the app (e.g., maintain, improve, or analyze functioning of app; perform network communications; authenticate users; cap frequency of advertising; protect security or integrity of user or app; facilitate legal or regulatory compliance; or allow app to be made available to user on user's device) and (2) prohibits the sharing of consumer data with subsequent third parties. App developers also do not have to notify users where there are disclosures to third parties of aggregate or de-identified data.

With respect to guidance from the software sector, the GSMA mobile app guidance asserts that users must be aware as soon as possible that data will be shared with third parties and notes that particular attention should be paid with respect to social networking/social media disclosures, targeted advertising functionality, and any app use by children and adolescents. And MOMs With Apps examines whether an app provider assesses third-party service providers' own privacy policies to ensure they also are COPPA-compliant.

KEY RECOMMENDATIONS FOR EDUCATIONAL INSTITUTIONS

Building from the examples in the financial services, healthcare, and software sectors, education policymakers, leaders, and practitioners should evaluate and consider a number of recommendations for developing and implementing student data privacy and security programs, policies, and procedures.[iv] The three overarching recommendations are (1) establishing ground rules for internal work; (2) appropriately managing third-party vendor relationships; and (3) committing to continuous improvement.[36] Concepts within each of these broad recommendations are explored in great detail, and policymakers and practitioners are encouraged to organize student data privacy and security efforts in light of the discussion that follows. Many education policymakers and practitioners already are incorporating at least some of these practices into their student data policies; that other industries also employ these practices reinforces their importance in ensuring the privacy and security of student information.

The adoption of the recommendations below will assist educators with establishing sustainable, repeatable, credible, defensible, and reliable processes for managing data use and controls, and with assuring students, parents, and other stakeholders of the commitment to student data privacy and security.

A. ESTABLISH THE INTERNAL GROUND RULES

Checklist for Recommendation 1
ESTABLISH THE GROUND RULES

- ✓ *Assess Your Data Collection Practices.*
- ✓ *Identify Your Security Objectives.*
- ✓ *Engage Key Education Administrators.*
- ✓ *Appoint a Data Leader with Responsibility for Privacy and Security Compliance.*
- ✓ *Conduct a Risk Assessment and Identify Security Needs.*
- ✓ *Ensure Internal Compliance.*

Assess Your Data Collection Practices. At the outset, districts and schools should examine their student data collection and use policies and practices. A student data mapping or inventory exercise should serve as a foundation for this work. Administrators should have an opportunity to determine whether current student data collections and uses are appropriate. The data inventory also will assist districts and schools with identifying data security risks and begin exploring safeguards and supports.

Identify Your Security Objectives. Districts and schools must identify security objectives when they establish policies and procedures to protect student data. Just as other sectors prompt data

[iv] As noted early in this paper, these recommendations apply also to state educational agencies that handle student data. They apply also to institutions of higher education as well as state early learning systems.

managers to set objectives for confidentiality, integrity, and availability of information, the education industry's objectives should conform to legal obligations regarding privacy and security and avoid unnecessary burdens on the appropriate, educational use of data. Attention is warranted for several situations, including the following: (1) the district or school's own, internal collection and use of student data; (2) the district or school's formal relationships with third-party contractors and vendors that involve disclosure and use of student data; and (3) the relationships between software providers and students (and educators) that implicate the collection of information from or about students. By striking the right balance, the security objectives can facilitate the appropriate use of student data to provide valuable supports, including via helpful education technology. Balancing appropriate student data accessibility and use to improve educational opportunities against the school or district's risk tolerances is critical for the identification of and commitment to respective security objectives.

Engage Key Education Administrators. Leadership from school and district administrators is critical for creating controls that ensure the adequate protection of student data. This work may require consideration of budgetary matters and redistribution of resources to support development and implementation of a data privacy and security infrastructure; the resolution of competing concerns and interests with respect to the collection and use of student data; and determinations regarding acceptable risk.

Appoint a Data Leader with Responsibility for Privacy and Security Compliance. A practice implemented in the financial services, healthcare, and software sectors involves tasking an individual or committee of individuals with primary oversight authority to ensure student data privacy and security program controls are effective. (For example, healthcare entities typically identify the individuals who will be directly responsible for responding to data incidents before the incidents occur.) The data leader coordinates activities associated with the adoption and implementation of privacy and security policies and procedures. And as additional legal requirements change, technology evolves, and new internal and external demands for student data arise, there will need to be close and careful scrutiny applied to each request for access and use of student data. A data privacy and security governance infrastructure led by a visible and accountable leader helps to ensure the proper stewardship of a state, district, or school privacy and data security program.

Conduct a Risk Assessment and Identify Security Needs. Before a district or school can develop or refine its data security program, it needs to take stock of current practices and resources.

- ***People, Processes, and Technology Inventories.*** Prior to conducting any risk assessment, the state, district, or school should review the people, processes, and technologies currently utilized for student data governance purposes.
    - "People" are individuals who play some role in the security of student data. "People" includes not only the data leader and administrators who set data use policies, but also educators to the degree they are involved in educational processes that involve sharing of student data (for example, teachers where they provide students with access to applications that solicit student data).
    - "Process" is the current methodology or practice applied to existing privacy and data security controls, policies, and procedures.

- Finally, "Technology" speaks both to (1) the technological resources available to contribute to the efficacy of data privacy and security controls and (2) the technology infrastructure used to house, access, and share student data (and, as guidance from the legal services sector demonstrates, this infrastructure is often mobile, with teachers and students accessing student data via mobile devices outside of the school building).

Districts and schools should examine each of these three pillars when inventorying their existing data resources. An inventory will reveal existing gaps that need attention in order to achieve the security objectives.

- ***Data-Mapping Exercises.*** In order to create and adopt the appropriate security safeguards, it is crucial to identify all of the data repositories of the educational institution. This evaluation must be broad and apply across the enterprise and to all systems. Unidentified and unsecured data can undermine student data privacy and security programs and the programmatic goals served by that program. Not knowing what data exists and the location of such data can be a difficult fact to defend in the event of data breach or other event that forces legitimate inquiry in the educational institution's data governance practices. Thoughtful security planning includes a determination of what data the district or school holds, the specific risks relating to such data, and the impact of data loss on all of the affected individuals. The understanding of the different data elements collected and used by the educational institution is important in the correct evaluation of the legal requirements which may apply to such collection and use.

Based on the people, processes, and technology in place, controls and approaches to achieve the desired security objectives may differ across schools and districts. By understanding the scope of data collection and gathering, along with the existing resources to achieve the security objective, a district or school can begin to focus on conducting the risk assessment.

Ensure Internal Compliance.

- ***Security Program Implementation***. Districts and schools should establish minimum data security compliance standards that correspond with and reinforce privacy policies that conform to federal and state laws. Drawing from established practices in all three sectors discussed above, a district or school's security program should include regular compliance audits, breach notification processes, and mitigation procedures. Security must include software/technology controls *and* people controls, the latter through background checks, training, and accountability mechanisms. The district and school also should establish an administrative system that can respond to complaints and requests for information and that can track disclosures of student data. Finally, as part of its security program, a school or district must identify storage and security protocols and work to enforce those protocols through oversight and education.[37]

- ***Employee Background Checks.*** Background screening of individual applicants is an established employment process across industries. The proper screening of employees from a data privacy and security perspective requires additional considerations and criteria as employees are screened for positions where access to sensitive data is readily available. Employees who have no access to sensitive student data may not require additional

screening beyond what would normally be required as part of the hiring process. By contrast, individuals who have unfettered access to sensitive student data may require additional screening and more thorough background checks. For example, this might include employment verification to ensure appropriate data stewardship in previous positions. The educational institution should only assign access to sensitive data to those individuals who need it to perform their assigned roles within the institution. The maintenance of a robust process to screen employees who have access to sensitive information can be an effective privacy and security control.

- ***Training***. Training is essential to an effective security program. Employees at every level, including teachers, should have a basic understanding and familiarity with the types of issues that create student privacy and data security risks. As with any employee training, there are endless possibilities for creative learning and messaging to help educate and familiarize all employees about good data privacy and data security practices. Many security breaches are not due to gaps in technical controls but occur as a result of a lack of human awareness of the privacy and security risks in the data environment and a lack of proper training with respect to these risks (e.g., someone clicks on a bad website and welcomes a virus). Ongoing awareness of data privacy and security risks is a critical component to establishing controls designed to protected student data.

- ***Monitoring, Auditing, and Reporting.*** Across sectors, monitoring is a critical element to any security program and often requires internal and external partners to be effective. The security program must be routinely tested, monitored, and updated for security threats. Continuous monitoring involves a real-time monitoring and updating process to defend against rapidly evolving and escalating threats. The provision of external monitoring services or utilization of internal resources for monitoring is a diligence hallmark of a sound data privacy and security program and can be effective in demonstrating the program is credible. Only through regular internal auditing of the security program by qualified individuals can the data privacy and security program maintain credibility. The development of the internal audit function is a key element to the development and maintenance of the program. Clear protocols must be in place to identify and report data breaches. In order to comply with legal obligations, clear policies should be in place to provide guidance on appropriate response and communication in the event of a breach.

- ***Accountability***. The drafting and publication of policies and procedures is ineffective unless there is an internal commitment to hold employees accountable for violations. Close coordination with human resources is critical in determining the ways in which data privacy and security policies and procedures will be enforced and how violations will be addressed. Consistent enforcement demonstrates a commitment to the maintenance of good privacy and security practices. Additionally, schools and districts that are able to demonstrate consistent enforcement of their programs, policies, and procedures can credibly defend their programs when inadvertent breaches occur or (in a worst case scenario) a rogue employee causes a breach scenario. Consistent enforcement can be used defensively and as an indicator of a serious and well-executed program.

B. EFFECTIVELY MANAGE THIRD-PARTY VENDOR RELATIONSHIPS

Checklist for Recommendation 2
ESTABLISHING THE GROUND RULES

- ✓ *Implement a Reasonable Vendor Approval and Governance Framework.*
- ✓ *Engage in a Risk Assessment Before Selecting a Third-Party Vendor.*
- ✓ *Use Qualified Counsel to Draft Contractual Assurances.*
- ✓ *Require Vendor Commitment to Compliance with the District or School's Privacy Policies.*
- ✓ *Assess Viability of Vendor's Own Internal Security Programs.*
- ✓ *Maintain the Right to Audit.*
- ✓ *Ensure Indemnification.*
- ✓ *Require Confidentiality and Data Stewardship.*
- ✓ *Establish Procedures for Breaches.*

Implement A Reasonable Vendor Approval and Governance Framework. Engaging third-party vendors brings risk into the student data environment. At the same time, vendors provide critical services to students, parents, and schools, offering (for example) valuable analytics data, data management services, data sharing tools, and parental engagement and communication services.

The guidance that follows is chiefly relevant for the development and execution of formal agreements between districts and schools and their contractors.[38] But policymakers should consider how the principles embodied in the recommendations below can be applied to informal arrangements, such as the arrangements created between app providers and students where students volunteer personal information in order to receive educational services. A comprehensive data privacy and security policy must address these instances and define how these relationships will be managed.

- ***Criteria and procedures for engaging third-party vendors***. Before addressing specific vendor relationships, districts and schools should establish criteria and procedures to evaluate proposed service providers, including those with formal contractual relationships and those used via informal contractual relationships (e.g., no-cost application based software that requires only click-through consent). Proactively setting expectations is important for legal compliance purposes and creates clear guidelines for all stakeholders who wish to utilize third-party vendor resources.

  Schools and districts need to think not only about their formal processes for contracting with vendors but also the less formal arrangements that are negotiated by individual educators and students themselves. Given the explosion of education technology, students, parents, and educators access a multitude of electronic resources as part of the educational process; technology tools can be downloaded directly as applications to wireless devices

and can provide tremendous value in the classroom environment. The extent to which these third-party application providers are adequately evaluated with respect to their handling and use of student data gathered should be a primary consideration. Adoption of a comprehensive framework and privacy and data security criteria for managing these relationships can provide valuable guidance to users and identify the factors which should be evaluated prior to technology use. The framework and guidance established to apply to all vendors must provide for consistent application, not unnecessarily stifle innovation in the utilization of new tools for student education, and be easily understood by all parties in the data-sharing ecosystem.

- ***Oversight of vendor activities*.** Just as districts and schools inventory their internal data practices, resources, and controls, a continual process to assess vendor activities should occur. A school or district should maintain and regularly update an inventory of all of its third-party vendors that access student information. Utilizing guidance from the healthcare sector, districts and policies could categorize vendors based on the extent of their overall access to student data as well as access to the most sensitive student data. As discussed below, audit and inventory activities as part of a district or school's ongoing monitoring of vendor activities may reveal concerns that warrant new requirements and action. Schools and districts may choose to establish a decision-making group to oversee vendors and ensure compliance.[39]

Engage in a Risk Assessment Before a Selecting Third-Party Vendor. As educational institutions engage third parties to perform certain services that require access to student data, the institutions should establish a set of criteria to properly evaluate the risk of providing a vendor with access to student data. Just as banks review the reputation of prospective contractors, districts and schools can conduct reference checks of vendors, examining their history of services for other clients. Technical advisors (personnel with a sophisticated understanding of information technology and data use) should be involved in this analysis. (This risk assessment framework and criteria can only be established upon the completion of the internal ground rules discussed above, including the risk assessment and identification of the security needs.)

Use Qualified Counsel to Draft Contractual Assurances. Districts and schools should engage qualified legal counsel and technical experts to draft agreements with third-party vendors, both as a matter of legal compliance and good policy. Provisions should be included on data security, governance, and ownership; the collection of data in accordance with the applicable legal requirements; the use, retention, disclosure, and destruction of data; the right of parents and students to access and modify their data; and more.

Require Vendor Commitment to Compliance with the District or School's Privacy Policies. Districts and schools should, at a minimum, require vendors, as part of a contractual relationship, to represent and warrant compliance with all applicable federal, state, and local laws, regulations, and rules that pertain to the possession or use of student data. District and schools also should require vendors to comply with their own privacy and information assurance policies.

Assess Viability of Vendor's Own Internal Security Programs. The third-party vendor should be required by written contract to maintain its own privacy and information security program, and conduct regular risk assessments of its security and information assurance practices. Schools and

districts may wish to include minimum standards for third-party vendors that mirror their own security objectives. At a minimum, the educational institution should obtain assurances that a third-party vendor maintains a security program that complies with any legal obligations that exist regarding the collection and sharing of student data. Schools and districts must have the ability to terminate third-party vendor relationships where the third-parties have breached these warranties.

Maintain the Right to Audit. The school or district should establish by contract the right to audit the vendor and the right to hire independent parties if necessary to conduct the audits. This right is critically important to ensuring the third-party vendor is serious about maintaining the data privacy and security of the information provided under the agreement. Third-party vendors that fail to agree to complete transparency with respect to data privacy and security practices should be viewed with skepticism and reconsidered.

Ensure Indemnification. Third-party vendors should be capable of providing broad-based indemnification for their failure to comply with applicable privacy laws; for their loss of data; for their negligence, gross negligence, or bad faith; and for any security breach involving the student data attributable to the vendor. Failure to secure indemnification for these failures by third-party vendors could have staggering political and economic ramifications for the school or district.

Require Confidentiality and Data Stewardship. The school or district should require a confidentiality provision ensuring adequate protection of student data. There should be specific written provisions to address protection, destruction, and return upon conclusion of the parties' relationship. In order to properly draft meaningful and enforceable confidentiality provisions, the education organization must engage in an evaluation of all institutional data and take steps to classify such data. Data classification would include establishing categories, such as information that is public, for internal use only, confidential, and restricted. Once the educational institution has classified the types of data in its possession, it can more easily establish criteria for its confidential treatment. Agreeing to these terms in advance has the added effect of determining how student data will be handled during and at the expiration of the agreement, substantially reducing the possibility that data will be mishandled upon termination of the agreement. Additionally, failure by the third-party vendor to abide by the terms of these provisions can entitle schools or districts to damages in the event these provisions are breached. Finally, with respect to the destruction and/or return of digital media, schools and districts should require secure digital media disposal ensures the deliberate and permanent removal or destruction of the data on a storage media device in order to render the data irrecoverable.

Establish Procedures for Breaches. Districts and schools should require a breach provision addressing, at a minimum, the procedures required for monitoring for breaches and for when a breach is discovered, including who is responsible for notifying affected parties and government authorities. The agreement should specify responsibilities for communications about the breach and involvement with law enforcement. Insurance requirements also should be negotiated.[40] Educational agencies should ensure that sufficient provisions exist in the vendor agreement to address any liability with respect to a privacy or security breach.

Guidance on Using Online Educational Services
U.S. Department of Education, Privacy Technical Assistance Center (PTAC)[41]

In February 2014, PTAC released *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* to address data privacy and security considerations in light of the information sharing, web-hosting, and telecommunication innovations that have enabled new education technologies. The resource examines relevant legal requirements under the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA) for online educational services and provides the following recommendations to school districts:

- Maintain awareness of federal, state, tribal, and local laws.
- Be aware of which online educational services are currently being used in your district.
- Have policies and procedures to evaluate and approve proposed online educational services.
- When possible, use a written contract or agreement that includes provisions on the following: security and data stewardship; data collection; data use, retention, disclosure, and destruction; data access; modification, duration, and termination; and indemnification and warranty.
- Extra steps are needed for click-wrap agreements, including checking amendment provisions, printing or saving the terms of service, and limiting authority to accept the terms of service.
- Be transparent with parents and students.
- Consider that parental consent may be appropriate.

C. COMMIT TO CONTINUOUS IMPROVEMENT IN DATA PRIVACY AND SECURITY EFFORTS AND TO TRANSPARENCY WITH RESPECT TO DATA PRACTICES

Checklist for Recommendation 3
COMMIT TO CONTINUOUS IMPROVEMENT AND DATA TRANSPARENCY

- ✓ Commit to Improvements and Updates to Data Security Policies and Procedures.
- ✓ Commit to Transparency and Communication.

Commit to Improvements and Updates to Data Security Policies and Procedures. A district or school's commitment to student data privacy and security must be continuous, and education policymakers and practitioners therefore should continually revisit and improve their data policies, programs, and procedures. This requires that district and school data leaders stay up-to-date on federal and state legislation, regulations, and guidance to ensure compliance with new requirements. Familiarity with new data regulations in other sectors also should be encouraged as new and promising practices may be gleaned from cross-industry analyses. Additionally, districts and schools should plan (1) to adjust their security programs when there are changes in data collection operations, (2) to respond to results in security testing and monitoring, and (3) to develop

additional safeguards as hackers and bad actors develop increasingly sophisticated techniques to effect data breaches.

Commit to Transparency and Communication. Districts and schools should increase awareness of their data policies and practices and inculcate a commitment to data privacy and security in all education stakeholders. Federal law requires certain notices to parents regarding data privacy, and states may establish their own requirements. Transparency makes sense not only for legal compliance purposes but also to create an informed culture in which stakeholders understand the value of student data collection and use and can trust that districts and schools are being responsible stewards of this information. Parents, students, teachers, and school officials should be aware of the district or school's data privacy and security commitments and efforts. Families are a critical constituency; providing those families with information about how their students' data are used and shared and with contact information for questions that arise can help reinforce the district or school's commitment to transparency and open communication.[42]

CONCLUSION

Policymakers are working to address issues of student data privacy and security in the 21st Century. A number of resources exist to support the development and implementation of effective approaches. Federal and state law requirements and attendant guidance from the education field offer one useful framework for this work. Additionally, education policymakers can consult the approaches employed by other sectors of the economy, adopted in light of legal regimes or industry self-regulation. By leveraging and adapting the best practices of sectors like financial services, healthcare, and software, the education field can develop effective and comprehensive policies for a digital age that protect student information while enabling educators to harness the tremendous promise of education data and technology to improve student outcomes.

ENDNOTES

[1] Borrowed, with permission, from Data Quality Campaign, *Federal Privacy Laws That Apply to Children and Education* (July 2014), http://dataqualitycampaign.org/files/Safeguarding%20Data%20Fed%20Privacy%20Laws.pdf; Data Quality Campaign, EducationCounsel, and Nelson Mullins, *Complying with FERPA and Other Federal Privacy and Security Laws and Maximizing Appropriate Data Use* (March 2013), http://www.educationcounsel.com/docudepot/articles/ Complying%20with%20FERPA%2003.2013.pdf.

[2] See, e.g., Lauren Tara Lacapra and Carrick Mollenkamp, *Security Breach Hits U.S. Card Processors, Banks*, REUTERS, March 30, 2012, http://www.reuters.com/article/2012/03/30/us-mastercard-breach-idUSBRE82T0VD20120330.

[3] Public Law 106-102 (1999); *see* Fed. Trade Comm'n, Bureau of Consumer Protection Business Center, *Gramm-Leach-Bliley Act*, http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

[4] In 2009, the Federal Trade Commission published a short-form financial privacy notice prototype; companies that use this prototype for their privacy notices are granted a safe harbor for purposes of compliance with the notice requirements of GLBA. The short-form prototype was developed in response to concerns that the lengthy notices mailed to consumers after GLBA was enacted were confusing. Consumer testing of the short-form prototype identified several important attributes for privacy disclosures – simplicity, good design techniques, neutral language and presentation, context, and standardization. Fed. Trade Comm'n, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), http://www.ftc.gov/sites/default/files/ documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobile privacyreport.pdf.

[5] *See infra* "Best Data Security Practices in the Financial Services Sector: Federal Trade Commission Safeguards Rule" (textbox); Federal Trade Commission, Bureau of Consumer Protection Business Center, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, http://www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

[6] U.S. Dep't of the Treasury, Office of the Comptroller of the Currency, *Risk Management Guidance* (Bulletin 2013-29) (OCT. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[7] *See* Payment Card Industry (PCI) Security Standards Council, *PCI SSC Data Security Standards Overview*, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

[8] PCI Security Standards Council, *PCI Data Security Standard: Requirements and Security Assessments Procedures* (November 2013), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

[9] *See* Fed. Trade Comm'n, Bureau of Consumer Protection, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (April 2006), http://www.business.ftc.gov/ documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

[10] 15 U.S.C. § 6802(b)(2).

[11] 12 CFR § 40.13(a)(i)(2). A third-party vendor also can disclose personal consumer data in order to carry out its business purpose (such as servicing transactions and complying with a legal requirement to disclose).

[12] *See, e.g.,* U.S. Dep't of Treasury, Office of the Comptroller of the Currency, *Third-Party Relationships* (Oct. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[13] *See, e.g.*, *Health Entities Across U.S. Report Data Breaches Affecting Millions*, IHEALTHBEAT, June 25, 2014, http://www.ihealthbeat.org/articles/2014/6/25/health-entities-across-us-report-data-breaches-affecting-millions; Patrick Ouellette, *Stanford Hospital, BAs Agree to $4 Million Breach Settlement*, HEALTH IT SECURITY, March 25, 2014, http://healthitsecurity.com/2014/03/25/stanford-hospital-agrees-to-4-million-breach-settlement/; Erin McCann, *HIPAA Data Breaches Climb 138 Percent*, HEALTHCARE IT NEWS, Feb. 6, 2014, http://www.healthcareitnews.com/news/hipaa-data-breaches-climb-138-percent.

[14] 42 U.S.C. § 300gg; 29 U.S.C. § 1181 *et seq.*; 42 U.S.C. § 1320d *et seq.*

[15] 45 CFR §§ 160, 164. *See also* U.S. Dep't of Health & Human Servs., Office for Civil Rights, *Summary of the HIPAA Privacy Rule* (May 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/ summary/privacysummary.pdf.

[16] *See generally* Affordable Health Care Act, Title I; Title I, sec. 2705(l)(3)(B)(iv).

[17] Ayla Ellison, *5 Tips for Protecting Patient Information & Responding to Healthcare Data Breaches*, BECKER'S HOSPITAL CIO, April 9, 2014, http://www.beckershospitalreview.com/healthcare-information-technology/5-tips-for-protecting-patient-information-responding-to-healthcare-data-breaches.html.

[18] *See, e.g.*, Deena Coffman, *The Fundamentals of Vendor Security*, BECKER'S HOSPITAL CIO, April 16, 2014, http://www.beckershospitalreview.com/healthcare-information-technology/the-fundamentals-of-vendor-security.html.

[19] *See Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules* (Omnibus Rule), 78 Fed. Reg. 5566 (Jan. 25, 2013), https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-

[20] 42 U.S.C. § 300gg; 29 U.S.C. § 1181 *et seq.*; 42 U.S.C. § 1320d *et seq.*

[21] *But see* Children's Online Privacy Protection Act, 15 U.S.C. § 6501; Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h. These statutes are discussed in this paper's introduction and below.

[22] Steve Cavanagh, *Draft Federal Data-Privacy Bill Targets Some Ed-Tech Practices, Silent on Others* (EDUC. WEEK, Jan. 29, 2015).

[23] *See* Fed. Trade Comm'n, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf (examining app practices with respect to privacy of information about children and finding that many apps share kids' information with third parties without disclosing these practices to parents).

[24] *See* Fed. Trade Comm'n, *Testing, Testing: A Review Session of COPPA and Schools* (Jan. 3, 2015), http://www.ftc.gov/news-events/blogs/business-blog/2015/01/testing-testing-review-session-coppa-schools; Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (July 16, 2014), http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions.

[25] *See* S.B. 1177 (2014), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?_bill_id=201320140SB1177; A.B. 1442 (2014), http://leginfo.legislature.ca.gov/ faces/billNavClient.xhtml?bill_id=201320140AB1442; A.B. 1584 (2014), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1584;

[26] *See supra* note 22; Michael D. Shear and Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES, Jan., 11, 2015, http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=0.

[27] Fed. Trade Comm'n, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[28] NTIA, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (July 25, 2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

[29] Calif. Office of the Attorney General, Joint Statement of Principles (Feb. 22, 2012), http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf. The six principles are as follows: (1) ensuring that apps collecting personal data conspicuously post their privacy policies with clear and complete information about how data is collected, used, and shared; (2) including in the application submission process for new or updated apps optional data fields where the app can provide the link to or text of its privacy policy; (3) providing a means for users to report app noncompliance with terms of service and laws; (4) responding to reported instances of noncompliance; and (5) working together to develop best practices for mobile privacy.

[30] California Dep't of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

[31] SSIA, *Best Practices for the Safeguarding of Student Information for Privacy and Security for Providers of School Services* (Feb. 24, 2014), http://siia.net/index.php?option=com_docman&task=doc_download&gid=4970&Itemid=318.

[32] Inside Mobile Apps, *ACT Debuts the App Privacy Icons* (Oct. 4, 2012), http://www.insidemobileapps.com/2012/10/04/act-debuts-the-app-privacy-icons/.

[33] For the complete list of guidelines, with implementation considerations, and examples see GSMA, *Privacy Design Guidelines for Mobile Application Development* (Feb. 22, 2012), http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development. *See also* Future of Privacy Forum and Center for Democracy & Technology, *Best Practices for Mobile Application Developers*, https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf.

[34] MOMs With Apps, *What Does It Mean for an App to Have the KNOW What's Inside Logo?*, https://momswithapps.com/about.

[35] kidSAFE, *kidSAFE Seal Program*, http://www.kidsafeseal.com/aboutourprogram.html.

[36] These recommendations also are consistent with remedies mandated by regulators as communicated in guidance after large-scale privacy and data security failures. *See, e.g.*, *United States v. ChoicePoint*, FTC File No. 052-3069 (N.D. Ga. Jan. 26, 2006) (requiring company to implement new procedures to ensure provision of consumer information reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year).

[37] *See* EducationCounsel, *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers* (March 2014), http://educationcounsel.com/docudepot/articles/EducationCounsel%20Guidance%20on%20State%20Student%20Privacy%20and%20Security%20Policies%20-%204838-6763-1641%20v%201.pdf.

[38] *See* Katz, *Contracting in a World of Data Breaches and Insecurity: Managing Third-Party Vendor Engagements* (LexisNexis May 2013), http://www.nelsonmullins.com/articles/katz-contracting-article.

[39] *See* Krivin et al., *Managing Third Party Risk in a Changing Regulatory Environment* (McKinsey & Company, May 2013), http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Risk/Working%20papers/46_Third_party_risk.ashx.

[40] Parks, *Data Breach Provisions in Outsourcing Contracts* (Nat'l Law Rev., June 24, 2014), http://www.natlawreview.com/article/data-breach-provisions-outsourcing-contracts.

[41] U.S. Dep't of Educ., Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (Feb. 2014), http://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

[42] *See* Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (July 16, 2014), http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions. The FTC recommends that schools consider providing parents with a list of the websites and online services whose collection it has consented to on behalf of the parents and should make available to interested parents the vendors' information collection and use policies. The FTC notes that some schools have implemented acceptable-use policies for Internet use to educate parents and students about how online services are being used in the classroom; the FTC recommended that schools post information about the sites they use on an online portal that they can direct parents to at the beginning of the school year.