Kentucky's 2015 Privacy Laws – Frequently Asked Questions

"HB 5" Questions and Answers

Q1: What is House Bill 5?

A: HB 5 (actually KRS 61.931, .932, .933, and .934 since it's no longer just a bill; it's the law) went into effect in January of 2015 and does 4 main things:

1. Requires the safety and security of personal information held by state agencies, including the Kentucky Department of Education (KDE), public school districts, colleges and universities AS WELL AS any entity/vendor/organization with which they have a contract (called "non-affiliated third parties" in the law). This means, essentially, that all Kentucky public agencies and their contracted vendors must implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches.
2. Defines, for Kentucky, "personal information."
3. Requires notification of specific state agencies and victims of a data breach. Any security and breach investigation procedures implemented by local school districts must be in accordance with regulations promulgated by the Kentucky Board of Education (KBE) – 702 KAR 1:170.
4. Lastly, HB 5 sets up some basic timelines and procedures that MUST be followed in the event of a data breach involving personal information.

Q2: Does HB 5 apply JUST to student data?

A: KRS 61.931 – 934 is not a law targeting only schools, students or K12 education. While HB 5 does apply to student data, it also applies to data about anyone, of any age, as long as it's held by a Kentucky state agency or an agency's contracted vendor. Schools naturally have personal information about students, but they also have personal information about employees, parents, other relatives, and so on. HB 5 applies to all of it, as long as it's considered "personal information."

Q3: What is "personal information?"

A: As defined by KRS 61.931 – 934, this is the information about a person that, if exposed, could very likely result in a data breach.

More precisely, "personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, IN COMBINATION WITH one (1) or more of the following data elements:

1. An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;

2. A Social Security number;

3. A taxpayer identification number that incorporates a Social Security number;

4. A driver's license number, state identification card number, or other individual identification number issued by any agency;

5. A passport number or other identification number issued by the United States government; or

6. Individually identifiable health information as defined in 45 C.F.R. sec. 160.103 except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;

Q4: Is the student ID number personal information?

A: It depends. While it meets the strict definition from KRS 61.931 – 934 of "other individual identification number issued by any agency," the student ID number exists only to ensure a unique identifier exists for each student within the Kentucky Student Information System (KSIS, or Infinite Campus) in case the student changes schools or districts. As such, it does not provide additional value beyond that purpose, unlike a Social Security Number or credit card number, which can be used not only for identification, but to obtain services, make purchases, and so on. By default, it's impossible to use a student ID number to access sensitive or confidential student information, like health or socio-economic status. Nor can one be used to make purchases. However, if a district decides to use the student number for additional purposes, then it might very easily become data that could cause a data breach if exposed and would be considered personal information.

The Family Policy Compliance Office, which is responsible for administering the Family Education and Rights Privacy Act (FERPA) has a very similar take. They have stated that a student identification number can be considered directory information, not PI. However, it would be directory information "only if the electronic identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the student's identity, such as a personal identification number (PIN), password, or other factor known or possess only by the student or authorized user."

If using the SSID to request assistance from KDE, KDE still encourages its use without other identifiers if at all possible.

Q5: Does KRS 61.931 – 934 impact my ability to enter into a contract with, well, anyone?

A: HB 5 does not prevent a district from entering into contracts, nor does it create a "safe list" of vendors. It does, however, require that any vendor (nonaffiliated third party) with whom personal information is shared will protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction. The vendor is also required to have

and keep up-to-date security and breach investigation procedures. In other words, they have to protect the data, but also have a plan for what happens if they suffer a breach.

Q6: What is a data breach?

A: A data breach occurs when personal information, which we discussed earlier, is exposed in an unauthorized manner which the district or district's vendor reasonably believes may compromise the "security, confidentiality, or integrity" of the data AND result in the "likelihood of harm to one (1) or more individuals." Essentially, if data are lost, stolen, changed or destroyed without authorization and there's a chance someone might get hurt or have their identity stolen, then it's a breach.

Some common examples of data breaches from Kentucky K-12 include:

- Accidentally emailing personal information to the wrong person or people
- Allowing papers with personal information on them to be disposed of in the trash, versus being shredded.
- Losing track of reports with personal information on them.
- Sharing one's username and password, which would grant access to personal information or systems with personal information on them.
- Becoming the victim of a phishing scheme or malware, where attackers have access to personal information.
- Having a laptop, USB drive, CD-ROM, or external hard drive containing personal information on it stolen from a residence or car.

Q7: What if my data are encrypted?

Encrypted data, if exposed WITHOUT the password or key required to unencrypt the data, would not be considered a data breach because the encryption protects the data.

Q8: What should I do if I suspect a data breach?

A: Every public school district should have their own internal processes for how to deal with a data breach, and if you don't know what that process is, now is the time to find out. Find out who in your school or district is the data breach contact person. Good bets are people in your district technology department, perhaps the CIO or DTC, or maybe it's the DPP. Ask that person what the official process is to report a data breach in your district, JUST IN CASE you are ever faced with one.

If you discover that your school or district has no official, documented data breach process, the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) has provided helpful resources to assist in the development of such a process.

http://ptac.ed.gov/document/data-breach-response-training-kit

The Kentucky Department of Education has also developed a document, the "Data Security and Breach Notification Best Practice Guide," to assist districts with complying with the notification requirements of HB 5 (KRS 61.931, .932, .933, and .934).

"HB 232" Questions and Answers

Q9: What is House Bill 232?

A: HB 232 also went into effect in 2015 and has 2 sections - KRS 365.732 and 365.734. The first section, .732, is not directed at schools, but benefits all Kentuckians by providing for consumer data breach protection. It also defines data breach and personally identifiable information for consumers, and requires that a vendor or business notify consumers when their data have been breached. Section 1 should be of great interest to all Kentuckians.

The second section, .734, directly impacts K12. It requires cloud computing service providers contracting with educational institutions to maintain security of student data and imposes limits what a cloud service provider can do with student data.

Q10: What are "student data?"

A: KRS 365.734 defines student data as including "the student's name, email address, email messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student."

More broadly, it means "any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services."

Q11: To whom does KRS 365.734 apply?

A: KRS 365.734 applies to cloud computing service providers – any person, entity or organization other than an educational institution that operates a cloud computing service. Two examples of cloud computing service providers in Kentucky are the statewide financial application and the statewide student information system. It is highly unlikely that student data would be contained within the financial application, but the student information system obviously contains a great deal of student data, meaning student information system should be much more concerned with this law than the financial application. Other examples might be library management software that is not housed locally, but stores data offsite, in the cloud, and classroom management apps.

Q12: What is a cloud computing service provider?

A: For the purposes of this law, a cloud computing service provider is a vendor, organization, or person, other than the educational institution, who provides a service via a network, like the Internet. In other words, the service is not maintained on-site.

Q13: What is a cloud computing service?

A: KRS 365.734 defines a cloud computing service as a "service that provides, and that is marketed and designed to provide, an educational institution with account-based access to online computing resources." Essentially if the service is accessed via a computer, tablet, phone, or any device via the Internet, it's considered a cloud computing service.

Q14: Are "apps" on my phone or computer cloud services?

A: Most likely. Cloud computing service providers aren't all large, statewide vendors. While Infinite Campus is obvious, consider all of the applications that get downloaded for "free" from mobile app stores or web sites. These, and most other apps, do, in fact, meet the definition of a cloud computing service provider. Many of them, such as learning management systems and classroom management systems require some amount of student data be uploaded in order to be useful, which means that teachers, schools and districts should be extra careful before committing to their use.

If student data, as defined by KRS 365.734, are shared/uploaded into these apps, there should be some assurance to the district that the provider is knowledgeable of and will abide by Kentucky's privacy legislation.

Q15: Does KRS 365.734 prevent me from downloading and using apps in my classroom?

A: No, but it does require that student data are protected from vendors, who might want to market to students or profit, from using or selling student data. Kentucky's law requires that a "cloud computing service provider that enters into an agreement to provide computing services to an educational institution shall certify in writing to the educational institution that it will comply" with KRS 365.734.

KDE interprets this to mean vendors must physically sign a legally binding agreement stating they will abide by the requirements of KRS 365.734. All of KDE's contracts with cloud service providers, such as Infinite Campus, have a signed agreement in place. Districts are not required to follow KDE's legal interpretation but are encouraged to seek signed agreements.

Q16: What, exactly, does KRS 365.734 require of cloud computing service providers?

A: In order to protect student data:

1. Cloud service providers cannot do anything with student data other than "providing, improving, developing, or maintaining" their cloud service…UNLESS
    a. they are assisting the school or district to conduct educational research as permitted by FERPA (Family Educational Rights and Privacy Act of 1974). They would be able to do this using FERPA's "School Official" exception. This is a commonplace action, but the district is required to inform parents when this exception is used.
    b. they have "express permission from the student's parent."

2. Cloud service providers cannot “process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertising purpose, and shall not sell, disclose, or otherwise process student data for any commercial purpose.”
3. Cloud service providers “shall certify in writing to the educational institution that it will comply with” with requirements of KRS 365.734.