

Laws, Statutory, Regulatory, and Contractual Security Requirements

Appendix A

CIPA, the Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

For more information, see: <http://www.fcc.gov/guides/childrens-internet-protection-act>

COPPA, the Children's Online Privacy Protection Act, regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information;

See www.coppa.org for details.

FERPA, the Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

For more information, see: <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

HIPAA, the Health Insurance Portability and Accountability Act, applies to organizations that transmit or store Protected Health Information (PHI). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

For more information, see: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/>

In general, schools are not bound by HIPAA guidelines.

Payment Card Industry Data Security Standard (PCI DSS) was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.

See www.pcisecuritystandards.org for more information.

PPRA, the Protection of Pupil Rights Amendment, affords parents and students who are 18 or emancipated minors (“eligible students”) certain rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

These include the right to the following:

Consent before students are required to submit to a survey that concerns one or more of the following protected areas (“protected information survey”) if the survey is funded in whole or in part by a program of the U.S. Department of Education (ED)–

1. Political affiliations or beliefs of the student or student’s parent;
2. Mental or psychological problems of the student or student’s family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating, or demeaning behavior;
5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
7. Religious practices, affiliations, or beliefs of the student or parents; or
8. Income, other than as required by law to determine program eligibility.

Receive notice and an opportunity to opt a student out of –

1. Any other protected information survey, regardless of funding;
2. Any non-emergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under State law; and
3. Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

For more information, see: <http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html>