Federal Data Protection Laws

This page provides a brief list of the most common federal data protection laws. For a more comprehensive list of key federal laws and regulations governing colleges and universities, please visit the Higher Education Compliance Alliance website to view the HECA Compliance Matrix.

The following federal laws apply to **how higher education institutions and non-governmental agencies collect and use data**.

- The **Family Educational Rights and Privacy Act of 1974 (FERPA)**: Protects students and their families by ensuring the privacy of student educational records. Educational records are agency or institution-maintained records containing personally identifiable student and educational data. FERPA applies to primary and secondary schools, colleges and universities, vocational colleges, and state and local educational agencies that receive funding under any program administered by the U.S. Department of Education.
    - See the U.S. Department of Education FERPA website for more information.
- The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**: Requires covered entities (typically medical and health insurance providers and their associates) to protect the security and privacy of health records. This law is often implicated in conversations about student data when institutions have a campus medical center and student medical records are integrated with student educational records (which are protected under FERPA).
    - See the U.S. Department of Health and Human Services HIPAA website for more information.
- The **Gramm Leach Bliley Act (GLBA)**: Applies to financial institutions and contains privacy and information security provisions that are designed to protect consumer financial data. This law also applies to how institutions collect, store, and use financial records (e.g., records regarding student tuition payments and/or financial aid) containing personally identifiable information.
    - See the U.S. Federal Trade Commission GLBA website for more information.
- The **Fair and Accurate Credit Transaction Act of 2003 (FACTA or "Red Flags Rule")**: Requires entities engaged in certain kinds of consumer financial transactions to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft. Like GLBA, this law applies to how institutions collect, store, and use student financial records.
    - See the U.S. Federal Trade Commission Red Flags Rule website for more information.

The following laws apply to **how the federal government collects and uses data**.

- The **Privacy Act of 1974**: Designed to protect the privacy of records created and used by the federal government. The law states the rules that a federal agency must follow to collect, use, transfer, and disclose an individual's personally identifiable information. The act also requires agencies to collect and store only the minimum information that they need to conduct their business. In addition, the law requires agencies to give the public notice about any records that it keeps that can be retrieved using a personal identifier (e.g., name or a Social Security Number).
    - See the U.S. Department of Justice Privacy Act website for more information.
- **E-Government Act of 2002**: Requires federal agencies to review and assess the privacy risks to their IT systems and publicly post privacy notices about their data collection practices. This law complements the Privacy Act of 1974 and was intended to promote access to electronic government resources. Under this law, an agency that collects personally identifiable information must conduct a privacy impact assessment before it collects that information. The privacy impact assessment must specify the data the agency will collect, how it is collecting those data, how it will use and/or share the data, whether individuals have the opportunity to consent to specific uses of the data (e.g., any use not otherwise permitted by law), how the agency will secure the data, and whether the data collected will reside in a system of records as defined by the Privacy Act.
    - See the U.S. Department of Justice E-Government Act website for more information.
- The **Federal Information Security Management Act of 2002 (FISMA)**: Designed to protect the security of federal information technology systems and the data contained within those systems. This law and its provisions apply to federal agencies and to contractors and affiliates of those agencies (such as educational institutions that receive a grant from a government entity). FISMA requires federal agencies to implement risk-based information security programs that conform to certain national standards. It also requires those programs to be independently reviewed each year.
    - See the U.S. Department of Homeland Security FISMA website for more information.

Questions or comments? Contact us.