Privacy Legislation Summary

Making sure it's secure.™

Protecting personal information is required by law, and Shred-it wants you to stay informed.

Privacy legislation is becoming more rigorous and continues to be strictly enforced. Organizations that fail to comply with applicable privacy legislation can incur severe penalties.

Here's a brief summary of current privacy legislation in the United States, along with the associated penalties for noncompliance.

Overview of U.S. Privacy Legislation

The Fair and Accurate Credit Transactions Act (FACTA)

FACTA provides consumers, companies, consumer reporting agencies and regulators with new tools to expand consumer access to credit, enhance the accuracy of consumer financial information and help fight identity theft.

- ✓ FACTA is administered by the Federal Trade Commission (FTC).
- ✓ Red Flag Rules require financial institutions and creditors to develop and use written identity theft prevention programs.
- ✓ Any person who possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access.

Penalties: Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of up to $1,000 per individual.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA requires health care organizations to have and maintain safeguards to prevent intentional or unintentional use or disclosure of protected health information.

Personal Health Information includes:

- ✓ medical records
- ✓ patient logs
- ✓ insurance
- ✓ billing
- ✓ any personally identifiable health information

Shredding prior to disposal is identified as an approved safeguard to prevent disclosure of protected health information.

Penalties: The most severe violation occurs when a person knowingly divulges patient information due to willful neglect and does not try to correct the situation. The fine for this violation is $50,000, with an annual maximum of $1.5 million.

Privacy Legislation Summary

Making sure it's secure.™

Overview of U.S. Privacy Legislation

The Health Information Technology for Economic and Clinical Health (HITECH) Act

includes rules that impact organizations that operate within HIPAA legislation.

The intention of the HITECH Act is to:

- ✓ increase enforcement of HIPAA rules
- ✓ impose mandatory penalties in a case-by-case basis for willful neglect.

Penalties: The most severe violation occurs when a person knowingly divulges patient information due to willful neglect and does not try to correct the situation. The fine for this violation is $50,000, with an annual maximum of $1.5 million.

Gramm-Leach-Bliley Act (GLB Act)

The GLB Act protects the privacy of consumer information held by financial institutions and requires companies to give consumers privacy notices that explain each institution's information-sharing practices. The act also provides consumers with the right to limit some sharing of their information.

Penalties: The penalties for violating the GLB Act are quite severe:

- ✓ A financial institution can be fined up to $100,000 for each violation.
- ✓ The officers and directors of the financial institution can be fined up to $10,000 for each violation.
- ✓ Criminal penalties include imprisonment for up to 5 years, a fine, or both.

Sarbanes-Oxley Act (SOX)

SOX was enacted to enhance corporate responsibility and financial reporting as well as combat corporate and accounting fraud.

Penalties: Noncompliance penalties range from the loss of an exchange listing to multimillion-dollar fines and imprisonment.

Economic Espionage Act (EEA)

EEA made it a criminal offense to steal trade secrets, defined as "all forms and types of financial, business, scientific, technical, economic or engineering information" that the owner has taken reasonable measures to keep secret and that is not known to the public. The legislation applies to information in any form.

Penalties: Companies that engage in economic espionage can be fined up to $10 million for stealing trade secrets for another government and up to $5 million for using stolen secrets for their own gain.

Privacy Legislation Summary

Making sure it's secure.™

Overview of U.S. Privacy Legislation

Safe Harbor Program

This is a voluntary program for companies that deal with data from European countries. Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Penalties: The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to $12,000 per day for violations.

Patriot Act

The Patriot Act was created to deter and punish terrorist acts in the United States and around the world, as well as for other purposes, including enhancing law enforcement investigator tools.

Penalties: Penalties in an amount equal to not less than two times the amount of the transaction, but not more than $1,000,000, on any financial institution or agency that commits a violation.

STATES AND COUNTIES

Many states, counties and municipalities have enacted their own legislation to protect personal information. To find out about local legislation that could affect your organization, visit shredit.com, and look for the Privacy Legislation section in our Resource Center at http://resource.shredit.com/legislativefactsheets.

Sources:

Bureau of Consumer Protection, Business Center, www.business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-actExport.gov
Export.gov, www.export.gov/safeharbor/eu/eg_main_018476.asp
Free Advice, www.criminal-law.freeadvice.com/criminal-law/criminal-law/economic-espioage.htm
Federal Trade Commission, www.ftc.gov
Lawyers.com, www. communications-media.lawyers.com/privacy-law/Gramm-Leach-Bliley-Act-and-Financial-Privacy.html
Sox-online, www.sox-online.com/basics.html
The United States Department of Justice, www.justice.gov
U.S. Department of Education, http://www.ed.gov/
U.S. Social Security Administration, www.socialsecurity.gov
International Association of Financial Crimes Investigators, www.iafci.org
Privacy Rights Clearinghouse, www.privacyrights.org
Identity Theft Clearinghouse, www.consumer.gov
Ponemon Institute, www.ponemon.org
Identity Theft Resource Center, www.idtheftcenter.org
http://www.hipaasurvivalguide.com/hitech-act-summary.php