Law Library

Table of Contents

Act to Regulate the Issue and Validity of Passports, And For Other Purposes, 1926 (as amended)

22 U.S.C. § 211a, Passports

Overview

This law provides that the U.S. Department of State is in charge of granting and issuing U.S. passports.

Helpful Tips

Passport records may consist of applications submitted for the issuance of a passport or other records such as a Consular Report of Birth, a Certificate of Witness to Marriage, a Certificate of Loss of Nationality, or a Consular Report of Death. These records are protected by the Privacy Act of 1974, 5 U.S.C. § 552a. Passport records do not include evidence of travel such as entrance/exit stamps, visas, residence permits, etc. Source: Order Copies of Passport Records
Executive Order 11295 designates and empowers the Secretary of State to exercise, without the approval, ratification, or other action of the President, the authority to designate and prescribe for and on behalf of the United States rules governing the granting, issuing, and verifying of passports.

Source: Executive Order 11295, Rules governing the granting, issuing, and verifying of United States passports

Regulations

22 C.F.R. Part 51

Executive Orders, Memoranda, and Directives

Rules Governing the Granting, Issuing, and Verifying of United States Passports, Exec. Order 11295 (31 FR. 10603, August 5, 1966) Available at: 22 U.S.C. § 211a, Passports and for further information at the National Archives – Executive Orders

Supplemental Material

Department of State

- Introduction to Passport Services
- Information Request Letters and Information Notices
- Release of Information from Passport Files
- Passport Amendments

Americans with Disabilities Act of 1990 (ADA) & Rehabilitation Act

Americans with Disabilities Act (ADA)

42 U.S.C. §§ 12101 et seq
42 U.S.C. § 12112(d) Discrimination

Rehabilitation Act (Rehab Act)

29 U.S.C. §§ 701 et seq (Chapter 16 Vocational Rehabilitation and Other Rehabilitation Services)

Overview

The ADA prohibits discrimination and guarantees that people with disabilities have the same opportunities as everyone else to participate in the mainstream of American life — to enjoy employment opportunities, to purchase goods and services, and to participate in State and local government programs and services. Modeled after the Civil Rights Act of 1964, which prohibits discrimination on the basis of race, color, religion, sex, or national origin – and Section 504 of the Rehabilitation Act of 1973 — the ADA is an "equal opportunity" law for people with disabilities.

The ADA, at 42 U.S.C. § 12112(d), generally prohibits medical examinations and inquiries of job applicants unless the inquiry is about the ability of the applicant to perform job related functions. The ADA does authorize medical examinations and inquiries by employers with regard to an employee's request for reasonable accommodation for a disability. In both instances, there are confidentiality requirements that attach to the records and information gathered.

The Rehabilitation Act of 1973 (also known as the "Rehab Act") prohibits discrimination on the basis of disability in programs run by federal agencies; programs that receive federal financial assistance; in federal employment; and in the employment practices of federal contractors. The standards for deciding if employment discrimination exists under the Rehab Act are the same as those used in Title I of the ADA.

The Rehab Act, at 29 C.F.R. § 791(f) and §793(d), provides that these sections of the ADA apply equally to those entities subject to the Rehab Act.

The Americans with Disabilities Act Amendments Act of 2008 (Public Law 110-325) (ADAAA) further amended the definition of "individual with a disability" and amended sections 12101, 12102, 12111 to 12114, 12201 and 12210 of the ADA and section 705 of the Rehab Act. The ADAAA also enacted sections 12103 and 12205a and re-designated sections 12206 to 12213.

Sources

- Introduction to the ADA
- Rehabilitation Act of 1973 (disability.gov)
- Titles I and V of the Americans with Disabilities Act of 1990 (ADA)
- The Rehabilitation Act of 1973 (EEOC)

Helpful Tips

The ADA, at 42 U.S.C. § 12112(d), generally prohibits medical examinations and inquiries of job applicants unless the inquiry is about the ability of the applicant to perform job related functions.

The ADA does authorize medical examinations and inquiries by employers with regard to an employee's request for reasonable accommodation for a disability. In both instances, there are confidentiality requirements that attach to the records and information gathered.
The Equal Employment Opportunity Commission (EEOC) issues government-wide regulations for implementing the ADA at 29 C.F.R. Part 1630. Except as otherwise provided in this part, this part does not apply a lesser standard than the standards applied under title V of the Rehabilitation Act of 1973 (29 U.S.C. §§ 790-794a, as amended), or the regulations issued by Federal agencies pursuant to that title. [29 C.F.R. § 1630.1(c)]

Regulations
29 C.F.R. Part 1630

Executive Orders, Memoranda, and Directives
Executive Order No. 13164 – Requiring Federal Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation

Supplemental Material
Equal Employment Opportunity Commission

- EEOC, Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation
- EEOC, Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act (ADA)
- EEOC, Enforcement Guidance: Workers' Compensation and the ADA
- EEOC, Enforcement Guidance on the Americans with Disabilities Act and Psychiatric Disabilities
- EEOC, Fact Sheet on Obtaining and Using Employee Medical Information as Part of Emergency Evacuation Procedures
- EEOC, Fact Sheet, The Family and Medical Leave Act, the Americans with Disabilities Act, and Title VII of the Civil Rights Act of 1964
- EEOC, The Mental Health Provider's Role in a Client's Request for a Reasonable Accommodation at Work
- EEOC, Questions & Answers about Persons with Intellectual Disabilities in the Workplace and the Americans with Disabilities Act (ADA)
- EEOC, Questions and Answers: The Application of Title VII and the ADA to Applicants or Employees Who Experience Domestic or Dating Violence, Sexual Assault, or Stalking
- EEOC, Helping Patients with HIV Infection Who Need Accommodations at Work

---

Aviation and Transportation Security Act of 2001
49 U.S.C. § 114 Transportation Security Administration
49 U.S.C. § 44909 Passenger Manifests
See also: Pub. Law 107-71

Overview
President Bush signed the Aviation and Transportation Security Act into law in November 2001, requiring screening conducted by federal officials, 100 percent checked baggage screening, expansion of the Federal Air Marshal Service and reinforced cockpit doors. The Transportation Security Administration (TSA) was created to oversee security in all modes of transportation.

Source

- Transportation Security Timeline

Regulations
19 C.F.R. Part 122 Subpart E
49 C.F.R. § 1540.107
49 C.F.R. Part 1560

Executive Orders, Memoranda, and Directives
Directive on Integration and Use of Screening Information To Protect Against Terrorism, HSPD-6 (Sept. 16, 2003)

Supplemental Material
U.S. Department of Homeland Security
Transportation Security Administration

- Travel Resources Page
- Passenger Name Record Privacy Policy

Bank Secrecy Act (BSA)
31 U.S.C. § 310

Overview
The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the Act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. It was passed by the Congress of the United States in 1970. The BSA is sometimes referred to as an anti-money laundering" law ("AML") or jointly as "BSA/AML." Several AML Acts, including provisions in Title III of the USA PATRIOT Act of 2001, have been enacted up to the present to amend the BSA. (See 31 USC 5311-5330 and 31 CFR Chapter X [formerly 31 CFR Part 103])

Sec. 31 U.S.C. § 310 (c)(2) requires the US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) to provide appropriate standards and guidelines for determining who is to be given access to the information maintained by FinCEN; what limits are to be

imposed on the use of such information; and how information about activities or relationships which involve or are closely associated with the exercise of constitutional rights is to be screened out of the data maintenance system.

When investigating potential money laundering or Bank Secrecy Act (BSA) violations, the key test (related statute test) is whether, under the facts and circumstances of the particular case, the money laundering and BSA provisions are considered related to the administration of the Internal Revenue laws.

Source

- FinCEN's Mandate from Congress

Helpful Tips

Sec. 31 U.S.C. § 310 (c)(2) Requirements Relating to Maintenance and Use of Data Banks

Regulations

31 C.F.R. Chapter X-Financial Crimes Enforcement Network, Department of the Treasury

Statutory Implementation Guidance

US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN)

Advisory, Maintaining the Confidentiality of Suspicious Activity Reports

Supplemental Material

US Department of the Treasury

Financial Crimes Enforcement Network (FinCEN)

- FinCEN's Mandate from Congress
- Answers to Frequently Questions about 31 C.F.R. Chapter X

Internal Revenue Service (IRS)

- Bank Secrecy Act

Census (Title 13)

Overview

The Census Bureau is bound by Title 13 of the United States Code. These laws not only provide authority for the work it does, but also provide strong protection for the information it collects from individuals and businesses. People sworn to uphold Title 13 are legally required to maintain the confidentiality of respondent data. Every person with access to respondent data is sworn for life to protect your information and understands that the penalties for violating this law are applicable for a lifetime.

Source

- Title 13 – Protection of Confidential Information

- Oath of Non-Disclosure

Supplemental Material
U.S. Census Bureau Data Protection

Children's Online Privacy Protection Act (COPPA)

Children's Online Privacy Protection Act (COPPA)
15 U.S.C. §§ 6501-6505

Overview
COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Source
- Federal Trade Commission "Children's Online Privacy Protection Rule ("COPPA")

Helpful Tips
Complying with COPPA: Frequently Asked Questions

Regulations
16 C.F.R. § 312

Statutory Implementation Guidance
OMB Memorandum M-03-22, Memorandum for Heads of Executive Departments and Agencies (Sept. 2003)

Supplemental Material
Federal Trade Commission "Children's Online Privacy Protection Rule ("COPPA")

Clinical Laboratory Improvement Amendments of 1988 (CLIA)

42 U.S.C. § 263a

Overview
The Clinical Laboratory Improvement Amendments of 1988 (CLIA) is an amendment to the Public Health Services Act in which Congress revised the federal program for certification and oversight of clinical laboratory testing. Two subsequent amendments were made after 1988. The law continues to be cited as CLIA '88 as named in legislation. In general terms, the CLIA regulations establish quality standards for laboratory testing performed on specimens from humans, such as blood, body fluid and tissue, for the purpose of diagnosis, prevention, or

treatment of disease, or assessment of health. The Centers for Medicare & Medicaid Services (CMS) regulates all laboratory testing (except research) performed on humans in the U.S. through CLIA. In total, CLIA covers approximately 254,000 laboratory entities. The Division of Laboratory Services, within the Survey and Certification Group, under the Center for Clinical Standards and Quality (CCSQ) has the responsibility for implementing the CLIA Program.

Source

- Clinical Laboratory Improvements Act (CMS)

Helpful Tips

CLIA regulations allow laboratories to give a patient, or a person designated by the patient, his or her "personal representative," access to the patient's completed test reports on the patient's or patient's personal representative's request. To align with this requirement, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule also provides individuals (or their personal representatives) with the right to access test reports directly from laboratories subject to HIPAA (CLIA-certified or CLIA-exempt laboratories). While patients can also get access to their laboratory test reports from their doctors, they have the option to obtain their test reports directly from the laboratory while maintaining strong protections for patients' privacy. The rules are issued jointly by three agencies within the U.S. Department of Health and Human Services: the Centers for Medicare & Medicaid Services (CMS), which is generally responsible for laboratory regulation under CLIA, the Centers for Disease Control and Prevention (CDC), which provides scientific and technical advice to CMS related to CLIA, and the Office for Civil Rights (OCR), which is responsible for enforcing the HIPAA Privacy Rule.

Sources

- HHS Strengthens Patients' Right to Access Lab Reports
- CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports (79 FR 7289, February 6, 2014)

Regulations

42 CFR Part 493
45 CFR Part 164

Supplemental Material

U.S. Department of Health and Human Services
Centers for Medicare and Medicaid Services

- Clinical Laboratory Improvement Amendments (CLIA)
- Centers for Disease Control and Prevention
    - Clinical Laboratory Improvement Amendments (CLIA)

Communications Assistance for Law Enforcement Act (CALEA)

47 U.S.C. §§ 1001-1010

Overview

In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA requires a "telecommunications carrier," as defined by the CALEA statute, to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment design and modify their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve. CALEA is limited to Telecommunications Carriers as defined by the Act and interpreted by the FCC. In addition, CALEA specifically exempts "Information Services", which includes many Internet based communications service providers, electronic storage providers and electronic messaging services.

Source

- Communications Assistance for Law Enforcement Act

Regulations

47 C.F.R. §§ 1.20000 – 1.20008

Supplemental Material

U.S. Department of Justice

Federal Bureau of Investigation

- Ask CALEA

Federal Communications Commission

- Communications Assistance for Law Enforcement Act

Communications Act of 1934

TITLE 47—TELECOMMUNICATIONS

47 U.S.C. §§ et seq 47 U.S.C. § 222, Privacy of Customer Information
47 U.S.C. § 338(i), Privacy Rights of Satellite Subscribers
47 U.S.C. § 551, Protection of Subscriber Privacy
47 U.S.C. § 605, Unauthorized Publication or Use of Communications

- See also, The Communications Act of 1934

Overview

The Communications Act of 1934 (the "Act") combined and organized federal regulation of telephone, telegraph, and radio communications. The Act created the Federal Communications Commission (FCC) to oversee and regulate these industries. The Act is updated periodically to add provisions governing new communications technologies, such as broadcast, cable and satellite television. The Act, as amended, is an expansive statue regulating U.S. telephone, telegraph, television, and radio communications. Its seven subchapters regulate virtually all aspects of the communications and broadcasting industry, including assignment of frequencies, rates and fees, standards, competition, terms of subscriber access, commercials, broadcasting in the public interest, government use of communications systems. The Act also provides for more detailed regulation and oversight via the establishment of the FCC.

Source

- The Communications Act of 1934

Regulations

47 C.F.R. Part 64 Subpart U – Customer Proprietary Network Information

Statutory Implementation Guidance

Federal Communications Commission (FCC)

- FCC Releases Proposed Rules to Protect Broadband Consumer Privacy, April 2016
- ISPs Should Take Reasonable Steps to Protect Privacy, May 2015
- Declaratory Ruling on Customer Proprietary Network Information in the Mobile Wireless Context, 2013
- Report and Order Adopting Rules to Address "Pretexting" and Other Matters, 2007
- Report and Order Adopting Implementing Rules, 2002

Note: most FCC rules are adopted by a process known as "notice and comment" rule-making. Under that process, the FCC gives the public notice that it is considering adopting or modifying rules on a particular subject and seeks the public's comment. The FCC considers the comments received in developing final rules.

Supplemental Material

Federal Communications Commission (FCC)

- Protecting Your Privacy: Phone and Cable Records

U.S. Department of Justice

- U.S. Attorneys' Manual, 47 U.S.C. § 605

Office of Justice Programs, Bureau of Justice Assistance

- The Communications Act of 1934

Consolidated Appropriations Act of 2005

Public Law No. 108-447 (see division H, title V, section 522)
Public Law No. 108-447

Overview

The Consolidated Appropriations Act of 2005 (the "Act") requires that each agency, subject to the Act:

- shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy. (Sec. 522(a))
- shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. (Sec. 522(b))
- shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. (Sec. 552(c))
- [a]t least every 2 years . . . shall have performed an independent, third party review of the use of information in identifiable form as the privacy and data protection procedures of the agency. (Sec. 522(d))
- [u]pon completion of a review, the Inspector General of an agency shall submit to the head of that agency a detailed report on the review. (Sec. 522(e))

Confidentiality of Medical Quality Assurance Records

38 U.S.C. §§ 5701 – 5728

Overview

Records and documents created by the Department of Veterans Affairs (VA) as part of a medical quality-assurance program are confidential and privileged and may not be disclosed to any person or entity except as provided in 38 U.S.C. § 5705.

Helpful Tips

The VA's National Center for Patient Safety (NCPS) has developed an internal, confidential, non-punitive system— the Patient Safety Information System. This reporting and analysis system allows users to electronically document patient safety information from across the VA so that "lessons learned" can benefit the entire system. A combined total of more than 1,000,000 root cause analysis reports and safety reports have been entered into the reporting system since it was established. Confidentiality is a key reason for the system's success. Because the Patient Safety Information System is part of a medical quality assurance program, the information within it is protected from disclosure under 38 U.S.C. § 5705.

Source

V.A. National Center for Patient Safety

Regulations

Regulations Text

38 C.F.R. § 17.500-511

Cybersecurity Information Sharing Act of 2015 (CISA)

6 U.S.C. §§ 149, 151, 1501-1510, 1521-1525, 1531-1533

Overview

On December 18, 2015, the President signed the Cybersecurity Act of 2015 (CISA) into law. Congress enacted CISA, Title I of the Cybersecurity Act, to direct the Department of Homeland Security (DHS)—in collaboration with other named agencies—to create a voluntary cybersecurity information sharing process that will protect participants from certain types of liability and encourage public and private entities to share cyber threat information in real-time while protecting the privacy and civil liberties of individuals.

Source

Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015"

Executive Orders, Memoranda, and Directives

- Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13691, (80 FR 9349, Feb. 13, 2015)
- Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13636 (78 FR 11737, February 12, 2013)
- Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21 (Feb. 2013)
- United States Cyber Incident Coordination, Presidential Policy Directive/PPD–41 (July 2016)

Supplemental Material

U.S. Department of Homeland Security

- Cybersecurity Information Sharing Act of 2015, June 15, 2016.
- Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, June 15, 2016.
- Guidance on Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015, February 16, 2016.
- Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government, June 15, 2016.

Drug Abuse Prevention, Treatment, and Rehabilitation Act

42 U.S.C § 290dd–2

Overview

Confidentiality of substance use disorder (alcohol and drug abuse) patient records is required under 42 U.S.C § 290dd–2 and 42 C.F.R Part 2. The statute and regulation require that records related to patient treatment of substance use disorders remain confidential subject to certain specific exceptions or patient consent to disclose such information. The statute extends to cover "any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States."

Source

Listening Session Comments on Substance Abuse Treatment Confidentiality Regulations

Helpful Tips

The Confidentiality of Alcohol and Drug Abuse Patient Records regulations, 42 C.F.R. Part 2, implement section 543 of the Public Health Service Act, 42 U.S.C. § 290dd-2, as amended by section 131 of the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act, Public Law 102-321. The regulations were promulgated as a final rule on July 1, 1975 (40 FR 27802).

The restrictions of these regulations upon the disclosure and use of drug abuse patient records were initially authorized by section 408 of the Drug Abuse Prevention, Treatment, and Rehabilitation Act. That section as amended was transferred by Public Law 98-24 to section 527 of the Public Health Service Act, which is codified at 42 U.S.C. § 290ee-3 (See 42 C.F.R. § 2.1<).

In addition, the restrictions of these regulations upon the disclosure and use of alcohol abuse patient records were initially authorized by section 333 of the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 (42 U.S.C. § 4582). The section as amended was transferred by Public Law 98-24 to section 523 of the Public Health Service Act which is codified at 42 U.S.C. § 290dd-3. (See 42 C.F.R. § 2.2).

Regulations

42 C.F.R. Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records

Supplemental Material

U.S. Department of Health and Human Services

Substance Abuse and Mental Health Services Administration (SAMHSA)

- Applying the Substance Abuse Confidentiality Regulations (2015)
- Frequently Asked Questions, Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE) (2010)

E-Government Act of 2002 (Section 208)

44 U.S.C. § 3501 note

- See also: Public Law 107-347

Overview

The availability of information, from personal information to public information, is made all the easier today due to technological changes in computers, digitized networks, internet access, and the creation of new information products. The E-Government Act of 2002 recognized that these advances also have important ramifications for the protection of personal information contained in government records and systems.

Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form. A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. The Act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns, reveal classified (i.e., national security) information, or sensitive (e.g., potentially damaging to a nation interest, law enforcement effort or competitive business interest contained in the assessment) information.

Source

E-government Act of 2002, Department of Justice

Helpful Tips

Several provisions of law were established in the E-Government Act of 2002 (Public Law 107-347), including the Federal Information Security Modernization Act of 2014 and the Confidential Information Protection and Statistical Efficiency Act of 2002. This page is specific to the privacy provisions of section 208 of the E-Government Act of 2002, codified at 44 U.S.C. § 3501 note, which pertain to privacy impact assessments and privacy protections on agency websites.

Statutory Implementation Guidance

Office of Management and Budget

- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 2003)
- OMB Memorandum M-03-18, Implementation Guidance for the E-Government Act of 2002 (Aug. 2003)

Executive Orders, Memoranda, and Directives
OMB Memorandum M-05-04, Policies for Federal Agency Public Websites (Dec. 2004)

Education Sciences Reform Act of 2002 (ESRA)

20 U.S.C. §§ 9501-9584

20 U.S.C. § 9573 Confidentiality

Overview
Institute of Education Sciences (IES). The mission of IES is to provide rigorous evidence on which to ground education practice and policy. This is accomplished through the work of its four centers: the National Center for Education Evaluation, the National Center for Education Research, the National Center for Education Statistics, and the National Center for Special Education Research.

Section 208 of the Education Sciences Reform Act of 2002 states, "All collection, maintenance, use, and wide dissemination of data by the Institute, including each office, board, committee, and center of the Institute, shall conform with the requirements of section 552a of title 5, United States Code, the confidentiality standards of subsection (c) of this section, and sections 444 and 445 of the General Education Provisions Act (20 U.S.C. §§ 1232g, 1232h)."

Further that "the Director shall ensure that all individually identifiable information about students, their academic achievements, their families, and information with respect to individual schools, shall remain confidential in accordance with section 552a of title 5, United States Code, the confidentiality standards of subsection (c) of this section, and sections 444 and 445 of the General Education Provisions Act (20 U.S.C. §§ 1232g, 1232h)."

The prohibitions of Section 9573 of Title 20 include:

- No person may use any individually identifiable information furnished…for any purpose other than a research, statistics, or evaluation purpose.
- No person may make any publication whereby the data furnished by any particular person…can be identified.
- No person may permit anyone other than the individuals authorized by the Director to examine the individual reports.

Electronic Communications Privacy Act of 1986 (ECPA)

18 U.S.C. §§ 1367, 2521, 2701 – 2712, 3117, 3121 – 3127
18 U.S.C. § 2510 – 2522 Wire and Electronic Communications Interception and Interception of Oral Communications (Wiretap Act)

18 U.S.C. §§ 2701-12. Stored Wire and Electronic Communications and Transactional Records Access (Stored Communications Act)
18 U.S.C. §§ 3121 – 3227 Pen Registers and Trap and Trace Devices

- See also: Public Law 99-508

Overview

The Electronic Communications Privacy Act (ECPA) of 1986 created additional privacy protections for stored electronic communications and updated the Federal Wiretap Act to cover electronic communications as well as oral and wire communications. Title II of the ECPA established a comprehensive system of protections for stored communications codified at 18 U.S.C. §§ 2701-2712 which has come to be referred to as the Stored Communications Act (SCA). The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically

Source: Justice Information Sharing, Electronic Communications Privacy Act of 1986

Helpful Tips

ECPA has three titles:

Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or 'procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." There are exceptions. Title I also prohibits the use of illegally obtained communications as evidence. [18 U.S.C. § 2515].

Title II of the ECPA, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. [18 U.S.C. §§ 2701-12].

Title III of the ECPA, which addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace. [18 U.S.C. §§ 3121 – 3227]

Amendments. The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008. Other acts have made specific amendments of lesser significance.

Source
Justice Information Sharing, Electronic Communications Privacy Act of 1986

Supplemental Material

U.S. Department of Justice

- Electronic Communications Privacy Act of 1986 (Public Law 99-508)
- Computer Crimes and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Chapter 3 (2009)

U.S. Mission to the European Union

Other Materials

- Big Data: Seizing Opportunities, Preserving Values

Fair Credit Reporting Act (FCRA)

15 U.S.C. § 1681

Overview

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. If your company meets the definition of a "consumer reporting agency" (CRA), if you furnish information to CRAs, or if you use that information for certain purposes, you may have obligations under the FCRA.

Source
Federal Trade Commission, Credit Reporting

Regulations

12 C.F.R. §1022
16 C.F.R. § 681
16 C.F.R. § 682

Statutory Implementation Guidance

U.S. Chief Human Capital Officers Council (CHCO)
Governmentwide Guidance to Ensure Fair Employment Opportunities for Applicants Who Are Unemployed or Facing Financial Difficulty Through No Fault of Their Own

Office of Personnel Management (OPM)
Notice No. 15-01: Reminder Regarding Requirements of the Fair Credit Reporting Act
Letter No. 98-02: Background Investigations

Supplemental Material

Consumer Financial Protection Bureau (CFPB)

- CFPB Bulletin 2013-09: The FCRA's requirement to investigate disputes and review "all relevant" information provided by consumer reporting agencies (CRAs) about the dispute
- CFPB Bulletin 2014-01: The FCRA's requirement that furnishers conduct investigations of disputed information
- CFPB Bulletin 2016-01: The FCRA's requirement that furnishers establish and implement reasonable written policies and procedures regarding the accuracy and integrity of information furnished to all consumer reporting agencies

Federal Trade Commission (FTC)

- Using Consumer Reports for Credit Decisions: What to Know About Adverse Action and Risk-Based Pricing Notices
- Using Consumer Reports: What Employers Need to Know
- Consumer Reports: What Information Furnishers Need to Know
- Disposing of Consumer Report Information? Rule Tells How
- Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft
- 40 Years of Experience with the Fair Credit Reporting Act: an FTC Staff Report with Summary of Interpretations
- Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues
- Advisory Opinion to Pickett (07-10-98)
- Advisory Opinion to Copple (06-10-98)
- Advisory Opinion to Goeke (06-09-98)

National Credit Union Administration (NCUA)

- Releasing Consumer Credit Information to Government Employers

---

Family Educational Rights and Privacy Act (FERPA)

20 U.S.C. § 1232g

Overview

FERPA protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.

FERPA permits educational agencies and institutions, such as Local Education Agencies (LEA) and their constituent schools, to disclose PII from education records to State Education Agencies (SEA) and other State educational authorities without a parent's prior consent under

certain conditions. For a review of the exceptions to the general prior consent rule in FERPA, see 34 CFR § 99.31. The most common exception that relates to disclosure to a State educational authority is found in §§ 99.31(a)(3) and 99.35. The disclosure must be in connection with:

- An audit or evaluation of Federal or State supported education programs; or
- The enforcement of or compliance with Federal legal requirements relating to such programs.

Information collected under this provision generally must be:

- Protected so that information is not disclosed to anyone other than the authorized representatives of the State educational authority (§ 99.35(b)(1)); and,
- Destroyed when no longer needed for the purposes listed above (§ 99.35(b)(2))

(Note: Federal entities, entities or individuals acting as the designated authorized representatives of the Attorney General, the Comptroller General, or the Secretary of Education, as well as other third parties receiving PII from education records without consent, generally must also protect the PII from unauthorized disclosure and comply with FERPA's recordation provisions for any authorized re-disclosure, and may only use it in accordance with FERPA and for the specific purposes for which it was disclosed.)

Sources

- Law and Guidance: Family Educational Rights and Privacy Act (FERPA)
- Family Educational Rights and Privacy Act (FERPA)

Helpful Tips

FERPA may also be known as Section 444 of the General Education Provisions Act.

Regulations

34 C.F.R. Part 99

Supplemental Material

U.S. Department of Education

- Family Policy Compliance Office
- Privacy Technical Assistance Center

Federal Agency Data Mining Reporting Act of 2007 (FADMRA)

42 U.S.C. § 2000ee-3

Overview

The Federal Agency Data Mining Reporting Act of 2007 (FADMRA) is contained in section 803 of the Implementing the Recommendations of the 9/11 Commission Act of 2007. The FADMRA provides that the head of each department or agency of the Federal Government that is engaged in any "pattern-based" data mining activity shall submit a report to Congress on all

such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made available to the public, except for an annex as described in subparagraph (c).

Federal Policy for the Protection of Human Subjects (Common Rule)

42 U.S.C. § 289

Overview

On July 12, 1974, the National Research Act (Pub. L. 93-348) was signed into law, thereby creating the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (the "Commission"). The current U.S. system of protection for human research subjects is heavily influenced by the Belmont Report, written in 1979 by the Commission.

In 1985, Congress enacted 42 U.S.C. § 289, providing that "The Secretary of the U.S. Department of Health and Human Services (HHS) shall by regulation require that each entity which applies for a grant, contract, or cooperative agreement under this chapter for any project or program which involves the conduct of biomedical or behavioral research involving human subjects submit in or with its application for such grant, contract, or cooperative agreement assurances satisfactory to the Secretary that it has established (in accordance with regulations which the Secretary shall prescribe) a board (to be known as an 'Institutional Review Board') to review biomedical and behavioral research involving human subjects conducted at or supported by such entity in order to protect the rights of the human subjects of such research."

The Federal Policy for the Protection of Human Subjects or the "Common Rule" was published in 1991 and codified in separate regulations by 15 Federal departments and agencies. The HHS regulations, 45 CFR part 46, include four subparts: subpart A, also known as the Federal Policy or the "Common Rule"; subpart B, additional protections for pregnant women, human fetuses, and neonates; subpart C, additional protections for prisoners; and subpart D, additional protections for children. A fifth subpart, subpart E, which concerns registration of Institutional Review Boards (IRBs) was added in 2009. For all participating departments and agencies, the Common Rule outlines the basic provisions for IRBs, informed consent, and Assurances of Compliance. Human subject research conducted or supported by each Federal department/agency is governed by the regulations of that department/agency. The head of that department/agency retains final judgment as to whether a particular activity it conducts or supports is covered by the Common Rule. If an institution seeks guidance on implementation of the Common Rule and other applicable Federal regulations, the institution should contact the department/agency conducting or supporting the research.

The HHS and fifteen other Federal departments and agencies have issued final revisions to the Federal Policy for the Protection of Human Subjects (the Common Rule). The Final Rule was published in the Federal Register on January 19, 2017. It implements new steps to better

protect human subjects involved in research, while facilitating valuable research and reducing burden, delay, and ambiguity for investigators.

Sources

- The Belmont Report
- Federal Policy for the Protection of Human Subjects ('Common Rule')
- HHS Historical Highlights
- Final Revisions to the Common Rule

Helpful Tips

The following terms in the Common Rule outline the regulation's applicability to privacy:

Section 102(f) of 45 CFR 46 defines "human subject" as "a living individual about whom an investigator (whether professional or student) conducting research obtains:

(1) Data through intervention or interaction with the individual, or
(2) Identifiable private information."

Private information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.

Regulations

U.S. Department of Health and Human Services
45 C.F.R. Part 46

See also, Basic HHS Policy for Protection of Human Research Subjects et al

Each agency that has implemented the Common Rule includes in its chapter of the Code of Federal Regulations section numbers and language that are identical to those of the HHS codification at 45 CFR part 46, subpart A. For the complete list and chapters of the CFR see: https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html.

Supplemental Material

U.S. Department of Health and Human Services
Office for Human Research Protections (OHRP)

- Final Revisions to the Common Rule
- Human Subjects Research Guidance
- Human Subjects Regulations Decision Charts
- Regulations and Policy Archived Materials

- National Health Registry Activities and 45 CFR part 46
- Regarding National Health Registries Activities, Letter from Ivor A. Pritchard, PhD, Senior Advisor to the Director of OHRP
- Guidance on the Genetic Information Nondiscrimination Act: Implications for Investigators and Institutional Review Boards
- Guidance on Research Using Coded Private Information or Specimens
- Guidance on Certificates of Confidentiality
- Collected Guidance on Vulnerable Populations

Office for Protection from Research Risks (OPRR)

- Issues to Consider in the Research Use of Stored Data or Tissues
- Guidance on Protections for Human Subjects in the National Institute of General Medical Sciences Human Genetic Mutant Cell Repository

Food and Drug Administration (FDA)

- Clinical Trials and Human Subject Protection

Federal Information Security Modernization Act of 2014 (FISMA)

44 U.S.C. Chapter 35 (44 U.S.C. §§ 3551-3558)

Overview

The Federal Information Security Modernization Act requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Source

OMB Circular No. A-130, Managing Information as a Strategic Resource (July 2016)

Helpful Tips

The Federal Information Security Modernization Act of 2014 (FISMA) was codified in the E-Government Act of 2002 as the Federal Information Security Management Act of 2002 (44 U.S.C. § 3501 note), and was reauthorized in 2014 (Pub. L. 113-283). The statute pertains to information security, which is defined as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and c) availability, which means ensuring timely and reliable access to and use of information.”

Source
44 U.S.C. § 3552(b)(3)

Executive Orders, Memoranda, and Directives

Office of Management and Budget

- OMB Circular No. A-130, Managing Information as a Strategic Resource (July 2016)

Supplemental Material

Office of Management and Budget (OMB)

- OMB Memorandum M-17-05, Fiscal Year 2016 – 2017 Guidance on the Federal Information Security and Privacy Management Requirements (Nov. 2016)
- Annual Report to Congress, Federal Information Security Management Act (Feb. 2015)

U.S. Department of Commerce

National Institute of Standards and Technology (NIST)

- Computer Security Division, Computer Security Resource Center, Federal Information Security Management Act (FISMA) Implementation Project

U.S. Department of Homeland Security

- FY 2016 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics
- Federal Information Security Modernization Act (FISMA) of 2014 information page

---

Federal Records Act of 1950 (FRA)

44 U.S.C. Chapter 31 et seq

Overview

The FRA provides that "the head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities." [44 U.S.C. § 3101]

The implementation of the FRA is overseen by the Archivist of the United States, who heads the National Archives and Records Administration (NARA). The Archivist provides "guidance and assistance to Federal agencies with respect to ensuring adequate and proper documentation of the policies and transactions of the Federal Government and ensuring proper records disposition." [44 U.S.C. § 2904]

Regulations

36 C.F.R. Chapter XII Subchapter B Records Management
36 C.F.R. Part 1236 Electronic Records Management

Food and Drug Administration Safety and Innovation Act (FDASIA)

21 U.S.C. §§ 301 et seq

- See also: Food and Drug Administration Safety and Innovation Act (Public Law No. 112-144)

Overview

FDASIA, which amended the Federal Food, Drug, and Cosmetic Act and was signed into law on July 9, 2012, expands the authorities of the U.S. Food and Drug Administration (FDA) and strengthens the agency's ability to safeguard and advance public health by:

- Giving the authority to collect user fees from industry to fund reviews of innovator drugs, medical devices, generic drugs, and biosimilar biological products;
- Promoting innovation to speed patient access to safe and effective products;
- Increasing stakeholder involvement in FDA processes; and
- Enhancing the safety of the drug supply chain.

Section 618 of FDASIA directed the Secretary of Health and Human Services, acting through the Commissioner of the FDA, and in consultation with the Office of the National Coordinator for Health Information Technology and the Chairman of the Federal Communications Commission, to develop a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework for health IT, including medical mobile applications, that promotes innovation, protects patient safety, and avoids regulatory duplication.

Sources

- Regulatory Information: Food and Drug Administration Safety and Innovation Act (FDASIA)
- Health IT Legislation: FDASIA

Helpful Tips

Section 618 of FDASIA imposed a one-time requirement that the U.S. Department of Health and Human Services (HHS) issue "a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication." The Office of Law Revision Counsel of the United States House of Representatives chose not to include this provision in the United States Code. The report was issued in April 2014.

Source

Food and Drug Administration Safety and Innovation Act (Public Law No. 112-144)

Supplemental Material

Food and Drug Administration, Federal Communications Commission, Office of the National Coordinator for Health Information Technology

- FDASIA Health IT Report Proposed Risk Based Regulatory Framework, April 2014

Foreign Intelligence Surveillance Act of 1978 and Amendments (FISA)

50 U.S.C. 1801 et seq

- See also: Public Law 95-511

Overview

FISA authorizes electronic surveillance and other activities to obtain foreign intelligence information. FISA has been amended repeatedly since 1978, including the FISA Amendments Act (FAA) of 2008 containing Section 702 (reflected in Title VII below) and most recently by the USA FREEDOM Act of 2015 (reflected in the various titles below). The titles of FISA are:

- Title I – Electronic Surveillance within the United States for Foreign Intelligence Purposes
- Title II – Conforming Amendments
- Title III – Physical Searches within the United States for Foreign Intelligence Purposes
- Title IV – Pen Registers and Trap and Trace Surveillance Devices for Foreign Intelligence Purposes
- Title V – Access to Certain Business Records for Foreign Intelligence Purposes
- Title VI – Reporting Requirement
- Title VII – Additional Procedures Regarding Certain Persons Outside the United States
- Title VIII – Protection of Person Assisting the Government

Helpful Tips

- Sec. 101. Definition. (50 U.S.C. § 1801)
- Sec. 102. Electronic surveillance authorization without court order;
- Sec. 301. Definitions. (50 U.S.C. § 1821)
- Sec. 302. Authorization of physical searches for foreign intelligence purposes. (50 U.S.C. § 1822)
- Sec. 303. Application for order. (50 U.S.C. § 1823)
- Sec. 304. Issuance of order. (50 U.S.C. § 1824)
- Sec. 305. Use of information. (50 U.S.C. § 1825)
- Sec. 401. Definitions. (50 U.S.C. § 1841)
- Sec. 402. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations. (50 U.S.C. § 1842)
- Sec. 501. Access to certain business records for foreign intelligence and international terrorism investigations. (50 U.S.C. § 1861)
- Sec. 601. Semiannual report of the Attorney General. (50 U.S.C. § 1871)
- Sec. 602. Declassification of Signification Decisions, Orders, and Opinions. (50 U.S.C. § 1872)

- Sec. 603. Annual Reports. (50 U.S.C. § 1873)
- Sec. 702. Procedures for targeting certain persons outside the United States other than United States persons. (50 U.S.C. § 1881a)
- Sec. 703. Certain acquisitions inside the United States targeting United States persons outside the United States. (50 U.S.C. § 1881b)
- Sec. 704. Other acquisitions targeting United States persons outside the United States. (50 U.S.C. § 1881c)
- Sec. 705. Joint applications and concurrent authorizations. (50 U.S.C. § 1881d)
- Sec. 706. Use of information acquired under this subchapter. (50 U.S.C. § 1881e)

Freedom of Information Act (FOIA)

5 U.S.C. § 552

- See also: Full Text of the FOIA Improvement Act of 2016 (Public Law No. 114-185)
- See also: U.S. Department of Justice Freedom of Information Act

Overview

Since 1967, the Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement.

Helpful Tips

U.S. Department of Justice

- Department of Justice Guide to the Freedom of Information Act

Supplemental Material

U.S. Department of Justice

- Office of Information Policy (OIP)
- FOIA.gov

Genetic Information Nondiscrimination Act of 2008 (GINA)

42 U.S.C. § 1320d-9, Application of HIPAA Regulations to Genetic Information
42 U.S.C. § 12112(d)(3), Employment Entrance Examination

- See also: Public Law 110-233

Overview

The Genetic Information Nondiscrimination Act (GINA) was signed into law on May 21, 2008. GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles.

Title I of GINA includes provisions that generally prohibit group health plans and health insurance issuers from discriminating based on genetic information. These provisions amend the Employee Retirement Income Security Act (ERISA), administered by the Department of Labor; the Public Health Service Act (PHS Act), administered by the Department of Health and Human Services (HHS); and the Internal Revenue Code (the Code), administered by the Department of Treasury (the Treasury) and the Internal Revenue Service (IRS). The Department of Labor has jurisdiction with respect to employment-based group health plans. HHS in conjunction with the States administers these provisions with respect to health insurance issuers. The Treasury and IRS administer these provisions with respect to employers. Title I of GINA also includes individual insurance market provisions under the PHS Act and privacy and confidentiality provisions under the Social Security Act, which are both within the jurisdiction of HHS.

With respect to privacy, statutory amendments were implemented under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act") in January 2013 to modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing section 105 of Title I of GINA. Specifically, the HIPAA Privacy Rule prohibits health plans from using or disclosing genetic information for underwriting purposes. The modifications also clarify that genetic information is health information and prohibit the use and disclosure of genetic information by covered health plans for eligibility determinations, premium computations, applications of any pre-existing condition exclusions, and any other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

Title II of GINA prohibits the use of genetic information in making employment decisions in any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoffs, training, fringe benefits, or any other term or condition of employment. It is enforced by the Equal Employment Opportunity Commission (EEOC).

Sources

- Frequently Asked Questions Regarding the Genetic Information Nondiscrimination Act
- What You Should Know: Questions and Answers about the Genetic Information Nondiscrimination Act (GINA) and Employment
- Health Information Privacy: Genetic Information

Helpful Tips

Sections 101(d), 102(f)(4), 103(d)(7), 104(b) and 201(4) define genetic information, with regard to any individual, as information about—

- such individual's genetic tests,
- the genetic tests of family members of such an individual, and
- the manifestation of a disease or disorder in family members of such an individual.

The term "genetic information" does not include information about the sex or age of any individual.

This definition was incorporated into the Employee Retirement Income Security Act (ERISA) at 29 U.S.C. § 1191b(d)); the Public Health Service Act at 42 U.S.C. § 300gg–91(d)); the Internal Revenue Code, 26 U.S.C. § 9832; and the Social Security Act at 42 U.S.C.§ 1395ss (Certification of Medicare supplemental health insurance policies).

Section 105 in Title I of GINA, at 42 U.S.C. § 1320d–9, provides for the privacy and confidentiality of genetic information within the context of the Social Security Act, through application of the HIPAA Privacy Rule to genetic information.

Section 206 in Title II of GINA provides for the confidentiality of genetic information in an employment setting, through the application of standards set forth in the Americans with Disabilities Act (ADA). It states that "An employer, employment agency, labor organization, or joint labor-management committee shall be considered to be in compliance with the maintenance of information requirements of this subsection with respect to genetic information subject to this subsection that is maintained with and treated as a confidential medical record under section 102(d)(3)(B) of the Americans With Disabilities Act (42 U.S.C. § 12112(d)(3)(B)).”

Regulations

26 C.F.R. § 54.9802-1
29 C.F.R. § 1630.14
44 C.F.R. Parts 160 and 164

Supplemental Material

U.S. Department of Labor

- Frequently Asked Questions Regarding the Genetic Information Nondiscrimination Act

U.S. Department of Health and Human Services (HHS)

- "'GINA': The Genetic Information Nondiscrimination Act of 2008, Information for Researchers and Health Care Professionals

Office for Human Research Protections (OHRP)

- Guidance on the Genetic Information Nondiscrimination Act: Implications for Investigators and Institutional Review Boards (Mar. 24, 2009)

U.S. Equal Employment Opportunity Commission (EEOC)

- What You Should Know: Questions and Answers about the Genetic Information Nondiscrimination Act (GINA) and Employment
- Memorandum of Understanding Between the U.S. EEOC and the U.S. Department Of Justice – Civil Rights Division Regarding ADA and GINA Employment Discrimination Charges Against State and Local Governments (July 23, 2015)
- Final Rule on Employer Wellness Programs and the Genetic Information Nondiscrimination Act (May 17, 2016)

U.S. Congressional Research Service

- The Genetic Information Nondiscrimination Act of 2008 and the Patient Protection and Affordable Care Act of 2010: Overview and Legal Analysis of Potential Interactions (Dec. 21, 2011)

Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

42 U.S.C. §§ 300jj et seq, 42 U.S.C. §§ 17901 et seq

- See also: American Recovery and Reinvestment Act of 2009 (Public Law 111-5, §§ 13001-13424, §§ 4001 – 4201)

Overview

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provides the U.S. Department of Health and Human Services (HHS) with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange. The HITECH Act amends Sections 3004 and 3005 of the Public Health Service Act to describe the processes for evaluation, adoption, and implementation of endorsed standards, implementation specifications, and certification criteria for health IT. Sections 13400-13411 of HITECH describe HHS's work to improve privacy and security provisions for electronic exchange and use of health information, and sections 4001-4201 of HITECH establish the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs to provide incentive payments for eligible professionals, hospitals, and critical access hospitals as they adopt, implement, upgrade, or demonstrate meaningful use of certified EHR technology.

Sources

- Health IT Legislation and Regulations
- Select Portions of the HITECH Act and Relationship to ONC Work

Helpful Tips

HITECH was enacted as part of the American Recovery and Reinvestment Act of 2009 and was signed into law on February 17, 2009.

The HHS Office for Civil Rights implemented important privacy and security provisions of HITECH, which lays out new and specific obligations for covered entities in the event of a data breach that include notifications to individual data subjects and in some instances, to the media. Please see the entry for the Health Insurance Portability and Accountability Act (HIPAA) for more complete information regarding privacy and security provisions for electronic exchange and use of health information.

HITECH established a process for the evaluation, adoption, and implementation of endorsed standards, implementation specifications, and certification criteria for health IT, and created an Office of the National Coordinator for Health Information Technology (ONC) within HHS to oversee this process, assisted by two advisory committees. The National Institute for Standards and Technology (NIST) conducts pilot testing for new technical standards. The resulting certification criteria regulations ensure all health IT presented for certification possess the relevant privacy and security capabilities.

HITECH also established the Medicare and Medicaid EHR Incentive Programs, which encourage health care organizations to adopt EHRs through a staged approach. Each stage contains core requirements in the final regulations that providers must meet, including privacy and security requirements.

Sources

- 45 C.F.R. Part 170
- 42 C.F.R. Part 412
- 42 C.F.R. Part 495
- 45 C.F.R. Part 160
- 45 C.F.R. Part 164

Regulations

2015 Edition Health Information Technology Certification Criteria – Final Rule
45 C.F.R. Part 170

Medicare and Medicaid Programs; Electronic Health Record Incentive Program – Stage 3 and Modifications to Meaningful Use in 2015 through 2017; Final Rules with Comment Period
42 C.F.R. Part 412
42 C.F.R. Part 495

General Administrative Requirements
45 C.F.R. Part 160

Security and Privacy
45 C.F.R. Part 160

Supplemental Material

U.S. Department of Health and Human Services

Office of Civil Rights

- Combined Regulation Text of All Rules

Office of the National Coordinator for Health Information Technology

- ONC Regulations Resources

Health Insurance Portability and Accountability Act of 1996 (HIPAA Breach Notification Rule)

42 U.S.C. § 17932

- See also: Health Information Technology for Economic and Clinical Health (HITECH) Act (Public Law 111-5, Div. A, title XIII, § 13402)
- See also: 45 C.F.R. §§ 164.400-414 (Subpart D)

Overview

Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (the "Act") requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of the U.S. Department of Health and Human Services (HHS) following the discovery of a breach of unsecured protected health information. In some cases, the Act requires covered entities also to provide notification to the media of breaches. In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach. Finally, the Act requires the Secretary to post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of HITECH and the Genetic Information Nondiscrimination Act (GINA).

Source

- Health Information Privacy: Breach Notification Rule

Helpful Tips

The U.S. Department of Health and Human Services added a new subpart D to part 164 of title 45 of the Code of Federal Regulations (CFR) to implement the breach notification provisions of section 13402 of the HITECH Act. In developing the interim final rule, the Department consulted closely with the Federal Trade Commission (FTC), which administers similar breach notification requirements on vendors of personal health records (PHRs) and their third party service providers under section 13407 of the HITECH Act. The interim final rule and FTC's Health Breach Notification Rule (74 FR 42962, published August 25, 2009) made clear that entities operating as HIPAA covered entities and business associates are subject to HHS', and not the FTC's, breach notification rule. Second, to address those limited cases where an entity may be subject to both HHS' and the FTC's rules, such as a vendor that offers PHRs to customers of a HIPAA covered entity as a business associate and also offers PHRs directly to the public, both

sets of regulations were harmonized by including the same or similar language, within the constraints of the statutory language. The HHS rule was finalized in 2013.

Source
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; Final Rule (78 FR 5566, January 25, 2013)

Supplemental Material

U.S. Department of Health and Human Services

- HIPAA Breach Notification Regulation History
- Summary of the HIPAA Breach Notification Rule
- Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individual

U.S. Department of Defense, Defense Health Agency (DHA) Privacy and Civil Liberties Office

- HIPAA Compliance within the Military Health Systems

U.S. Federal Trade Commission (FTC)

- Complying with the FTC's Health Breach Notification Rule
- Mobile Health Apps Interactive Tool

Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy Rule)

Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)
45 C.F.R. Part 160
45 C.F.R. Part 164 Subparts A and E

Overview

The HIPAA Privacy Rule, adopted by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Sources

- Health Information Privacy: The HIPAA Privacy Rule
- The Health Insurance Portability and Accountability Act of 1996

Helpful Tips

The complete suite of HIPAA Administrative Simplification Regulations can be found at 45 C.F.R. Part 160, Part 162, and Part 164, and includes:

- Transactions and Code Set Standards
- Identifier Standards
- Privacy Rule
- Security Rule
- Enforcement Rule
- Breach Notification Rule

Source

Health Information Privacy, Complete Text of All Rules

Supplemental Material

U.S. Department of Veterans Affairs, Office of General Counsel

- The HIPAA Privacy Rule
- Summary of the HIPAA Privacy Rule
- HIPAA Guidance Materials
- Special Topics in Health Information Privacy
- HIPAA FAQs for Professionals
- HIPAA Privacy Rule and Public Health; Guidance from CDC and the U.S. Department of Health and Human Services
- HHS National Institutes of Health (NIH), HIPAA Privacy Rule, Information for Researchers

U.S. Department of Defense, Defense Health Agency (DHA)

- HIPAA Information

U.S. Department of Defense, Defense Health Agency (DHA) Privacy and Civil Liberties Office

- HIPAA Compliance within the Military Health Systems

Health Insurance Portability and Accountability Act of 1996 (HIPAA Security Rule)

Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)

- See also: 45 C.F.R. Part 160

- See also: 45 C.F.R. §§ 164.102-106 and §§ 164.302-318

Overview

The HIPAA Security Rule, adopted by the U.S. Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act of 1996 establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Sources

- Health Information Privacy, The Security Rule
- Health Information Portability and Accountability Act of 1996

Helpful Tips

The complete suite of HIPAA Administrative Simplification Regulations can be found at 45 C.F.R. Part 160, Part 162, and Part 164, and includes:

- Transactions and Code Set Standards
- Identifier Standards
- Privacy Rule
- Security Rule
- Enforcement Rule
- Breach Notification Rule

Source

Health Information Privacy, Combined Text of All Rules

The Administrative Simplification provisions of HIPAA, Title II required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI). The text of the final regulation can be found at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

Supplemental Material

U.S. Department of Health and Human Services (HHS)

- The Security Rule
- Summary of the HIPAA Security Rule

- 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
- Security Rule Guidance Material
- Final Guidance on Risk Analysis
- Remote Use
- Your Mobile Device and Health Information Privacy and Security
- HHS, Centers for Disease Control and Prevention (CDC), National Program of Cancer Registries, Data Security Guidelines for Cancer Registries
- National Institutes of Health (NIH), Health Services Research Information Central (HSRIC), Privacy/Security and Research with Electronic Health Records

U.S. Department of Veterans Affairs (VA)

- VA Mobile, Data Security

U.S. Department of Defense, Defense Health Agency (DHA) Privacy and Civil Liberties Office

- HIPAA Compliance within the Military Health Systems

Homeland Security Act of 2002

6 USC § 101 et seq

- See also: Pub. Law 107-296 and the Office of the Director of National Intelligence Legal Reference Book

Overview

The Homeland Security Act of 2002 charges the Department of Homeland Security (DHS) Chief Privacy Officer with primary responsibility for ensuring that privacy considerations and protections are integrated into all DHS programs, policies, and procedures. The Chief Privacy Officer serves as the principal advisor to the DHS Secretary on privacy policy.

The activities of the Privacy Office serve to build privacy into departmental programs.

Sources

- Department of Homeland Security, Privacy Office, "Fiscal Year 2016 Semiannual Report to Congress: For the period October 1, 2015 – March 31, 2016," July 6, 2016
- DHS, Authorities and Responsibilities of the Chief Privacy Officer

Helpful Tips

More information can be found in the following resources:

- Sec. 222. Privacy Officer. (6 U.S.C. § 142)

- Sec. 1004. Information Security and Privacy Advisory Board. (15 U.S.C. § 278g-4)
- Sec. 1601. Retention of security sensitive information authority at Department of Transportation. (49 U.S.C. § 40119)

Subsequent amendments, Pub.L. 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007

Executive Orders, Memoranda, and Directives

- United States Intelligence Activities, Exec. Order No. 12333 (46 FR 59941, Dec. 08, 1981), amended by Exec. Order 13284 (68 FR 4057, Jan. 28, 2003), Exec. Order 13355 (69 FR 53593, Sept. 1, 2004), and Exec. Order 13470 (73 FR 45325, Aug. 4, 2008)
- Further Strengthening the Sharing of Terrorism Information to Protect Americans, Exec. Order No. 13388 (70 FR 62023, Oct. 27, 2005)
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 2016)

Immigration and Nationality Act of 1952 (INA)

8 U.S.C. §§ 1101 et seq

- See also: Immigration and Nationality Act (U.S. Citizenship and Immigration Services)

Overview

The Immigration and Nationality Act, or INA, was created in 1952. The Act has been amended many times over the years, but is still the basic body of immigration law. The INA is divided into titles, chapters, and sections. Although it stands alone as a body of law, the Act is also contained in the United States Code (U.S.C.). When browsing the INA or other statutes you will often see reference to the U.S. Code citation. For example, Section 208 of the INA deals with asylum, and is also contained in 8 U.S.C. 1158. Although it is correct to refer to a specific section by either its INA citation or its U.S. Code citation, the INA citation is more commonly used.

Source

- Immigration and Nationality Act

Helpful Tips

Enforcement of the INA, including protection of confidentiality and privacy, involves multiple agencies, including but not limited to the U.S. Department of State, Customs and Border Protection, U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, and the U.S. Department of Labor.

Regulations

8 C.F.R. et seq

22 C.F.R. et seq (Vol. 1 (Parts 1-299) and Vol 2. (Parts 300-1799))

Executive Orders, Memoranda, and Directives

- Suspension of Entry as Immigrants and Nonimmigrants of Persons Who Participate in Serious Human Rights and Humanitarian Law Violations and Other Abuses, Proclamation No. 8697 (76 FR 49275, Aug. 4, 2011)
- Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions, Proclamation No. 8693 (76 FR 44751, July 25, 2011)
- Directive on Integration and Use of Screening Information To Protect Against Terrorism, HSPD-6 (Sept. 16, 2003)

Supplemental Material

Department of State

- Foreign Affairs Manual (FAM) Provisions at 9 FAM 601.6, Maintaining Visa Files, Records and Information
- About Visas – The Basics

Department of Homeland Security

- Violence Against Women Act (VAWA) Confidentiality Provisions at DHS

U.S. Citizenship and Immigration Services (USCIS)

- Policy Manual, Vol. 1, Chap. 5, General Policies and Procedures, Part A., Customer Service, Privacy and Confidentiality in Customer Service
    - Tip: The USCIS Policy Manual is the agency's centralized online repository for USCIS's immigration policies
- E-Verify – Our Commitment to Privacy, U.S. Citizenship and Immigration Services (USCIS)

U.S. Immigration and Customs Enforcement

- Office of Information Governance and Privacy (ICE)

Department of Labor

- Popular Topics: Immigration

Implementing Recommendations of the 9/11 Commission Act of 2007

6 U.S.C. 101 et seq

- See also: Pub. Law 110-153 and the Office of the Director of National Intelligence Legal Reference Guide

Overview

This Act amended section 1016 of Intelligence Reform and Terrorism Prevention Act (IRTPA) and amended the Homeland Security Act of 2002 to expand and further refine the scope of the Information Sharing Environment (ISE).

Helpful Tips

More information can be found in the following resources:

- Sec. 504. Information sharing. (6 U.S.C. § 485)
- Sec. 511. Department of Homeland Security State, Local, and Regional Fusion Center Initiative. (6 U.S.C. § 121 et seq)
- Sec. 801. Modification of authorities relating to Privacy and Civil Liberties Oversight Board. (5 U.S.C. § 601 note)
- Sec. 802. Department Privacy Officer. (6 U.S.C. § 142)
- Sec. 803. Privacy and Civil Liberties Officers. (42 U.S.C. § 2000ee-1)
- Sec. 804. Federal Agency Data Mining Reporting Act of 2007. (42 U.S.C. § 2000ee-3)
- Sec. 1606. Appeal and redress process for passengers wrongly delayed or prohibited from boarding a flight. (49 U.S.C. § 44926)

Individuals with Disabilities Education Act (IDEA)

20 U.S.C. §§ 1400 et seq
20 U.S.C. § 1417(c), Confidentiality

Overview

IDEA is a law ensuring services to children with disabilities throughout the nation. IDEA governs how states and public agencies provide early intervention, special education and related services to more than 6.5 million eligible infants, toddlers, children and youth with disabilities. Infants and toddlers with disabilities (from birth through age 2) and their families receive early intervention services under IDEA Part C. Children and youth (from age 3 through age 21) receive special education and related services under IDEA Part B. Parts B & C require that the Secretary of the U.S. Department of Education shall take appropriate action, in accordance with section 444 of the General Education Provisions Act (GEPA), to ensure the confidentiality of any personally identifiable data, information, and records collected or maintained by the Secretary and by State educational agencies (SEA) and local educational agencies (LEA).

Sources

- Building the Legacy: IDEA 2004
- IDEA and FERPA Confidentiality Provisions

Regulations

- Part B: 34 C.F.R. Part 300
- Part C: 34 C.F.R. Part 303

Supplemental Material

U.S. Department of Education

- IDEA and FERPA Confidentiality Provisions

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

Pub. L. 108-458
Office of the Director of National Intelligence Legal Reference Book

Overview

IRTPA addresses many different facets of information gathering and the intelligence community. IRPTA's eight titles reflect its broad scope:

- Title I – Reform of the Intelligence Community
- Title II – Federal Bureau of Investigation
- Title III – Security Clearances
- Title IV – Transportation Security
- Title V – Border Protection, Immigration, and Visa Matters
- Title VI – Terrorism Prevention
- Title VII – Implementation of 9/11 Commission Recommendations
- Title VIII – Other Matters, including a requirement that the Department of Homeland Security ensure that the civil rights and civil liberties of persons are not diminished by efforts, activities, and programs aimed at securing the homeland.

Helpful Tips

More information can be found in the following resources:

- Sec. 1011. Reorganization and improvement of management of intelligence community. (50 U.S.C. § 3021 et seq)
- Sec. 103D. Civil Liberties Protection Officer. (50 U.S.C. § 3029)
- Sec. 1016. Information sharing. (6 U.S.C. § 485)
- Sec. 1061. Privacy and Civil Liberties Oversight Board. (42 U.S.C. § 2000ee et seq)
- Sec. 1062. Sense of Congress on Designation of Privacy and Civil Liberties Officers. (Pub.L. 108-458)
- Sec. 4012. Advanced airline passenger prescreening. (49 U.S.C. § 44903(j)(2))
- Sec. 6002. Additional semiannual reporting requirements under the Foreign Intelligence Surveillance Act of 1978. (50 U.S.C. § 1871)
- Sec. 7212. Driver's licenses and personal identification cards. (49 U.S.C. § 30301 note)
- Sec. 8302. Mission of Department of Homeland Security. (6 U.S.C. § 111(b)(1))
- Sec. 8303. Officer for Civil Rights and Civil Liberties. (6 U.S.C. § 345(a))
- Sec. 8304. Protection of civil rights and civil liberties by Office of Inspector General. (5 U.S.C. App. Inspector General Act of 1978)
- Sec. 8305. Privacy officer. (6 U.S.C. § 142)

Executive Orders, Memoranda, and Directives

- United States Intelligence Activities, Exec. Order No. 12333 (46 FR 59941, Dec. 08, 1981), amended by Exec. Order 13284 (68 FR 4057, Jan. 28, 2003), Exec. Order 13355 (69 FR 53593, Sept. 1, 2004), and Exec. Order 13470 (73 FR 45325, Aug. 4, 2008)
- Further Strengthening the Sharing of Terrorism Information to Protect Americans, Exec. Order No. 13388 (70 FR 62023, Oct. 27, 2005)
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 2016)

Internal Revenue Code (Tax Code)

26 U.S.C. §§ et al
26 U.S.C. § 6103 Confidentiality and disclosure of returns and return information
26 U.S.C. § 6713 Disclosure or use of information by preparers of returns
26 U.S.C. § 7213 Unauthorized disclosure of information
26 U.S.C. § 7213a Unauthorized inspection of returns or return information

- See also: Internal Revenue Service Laws and Regulations

Overview

Taxpayers have the right to expect that any Internal Revenue System (IRS) inquiry, examination, or enforcement action will comply with the law and be no more intrusive than necessary, and will respect all due process rights, including search and seizure protections and will provide, where applicable, a collection due process hearing.

Taxpayers have the right to expect that any information they provide to the IRS will not be disclosed unless authorized by the taxpayer or by law. Taxpayers have the right to expect appropriate action will be taken against government officers and employees, tax return preparers, and others who wrongfully use or disclose taxpayer return information.

Source
Your Rights as a Taxpayer

Helpful Tips

The Internal Revenue Code § 6103(h)(1) provides that returns and return information shall, without written request, be open to inspection by or disclosure to officers and employees of the Department of the Treasury whose official duties require such inspection or disclosure for tax administration purposes. The Internal Revenue Code § 6103(b)(4) provides that the term “tax administration” means the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes (or equivalent laws and statutes of a state) and tax conventions to which the United States is a party.

Internal Revenue Code § 6713 imposes a civil penalty of $250 on any person who is engaged in the business of preparing, or providing services in connection with the preparation of returns of tax, or any person who for compensation prepares a return for another person, and who "Discloses any information furnished to him for, or in connection with, the preparation of any such return, or Uses any such information for any purpose other than to prepare, or assist in preparing, any such return. Imposition of the penalty under [this section] does not require that the disclosure be knowing or reckless as it does under Internal Revenue Code § 7216." 26 U.S.C. §7216 is a criminal provision enacted by the U.S. Congress in 1971 that prohibits preparers of tax returns from knowingly or recklessly disclosing or using tax return information. A convicted preparer may be fined not more than $1,000 or imprisoned not more than one year or both, for each violation.

Returns and return information may be used or disclosed to initiate or conduct a money laundering investigation if the investigation is considered for tax administration purposes according to 26 U.S.C. § 6103(b)(4). When investigating potential money laundering or Bank Secrecy Act (BSA) violations, the key test (related statute test) is whether, under the facts and circumstances of the particular case, the money laundering and Bank Secrecy Act provisions are considered related to the administration of the Internal Revenue laws. Data collected by IRS personnel pursuant to their enforcement responsibilities under the BSA in a "pure" Title 31 investigation are not return information under section 6103. In a "pure" Title 31 investigation, i.e., where no Title 26 related statute determination has been made, the information is subject to the disclosure rules found at 31 U.S.C. § 5319 et seq. When Title 31 has been determined to be a statute related to tax administration for Section 6103 purposes, the entirety of the information is covered by Section 6103 because it was received by the Secretary for the purpose of determining some individual's liability or potential liability under the Code.

Sources

- IRS: Bank Secrecy Act
- IRS: Bank Secrecy Act – Disclosure
- In 1997, the Taxpayer Browsing Protection Act "amend[ed] the Internal Revenue Code of 1986 to prevent the unauthorized inspection of tax returns or tax return information

Regulations

- 26 C.F.R. § 301.7216.1 See pages 556 – 558
- See also Internal Revenue Service Laws and Regulations

Statutory Implementation Guidance

U.S. Department of Treasury

- Treasury Department Circular 230 (Revised 6-2014), Rules Governing Practice Before the Internal Revenue Service

Internal Revenue Service (IRS)

- Internal Revenue Procedure 2007-40, Internal Revenue Bulletin: 2007-26, Rev. Proc. 2007-40, June 25, 2007

Supplemental Material

U.S. Department of Treasury, Internal Revenue Service (IRS)

- Disclosure & Privacy Law Reference Guide
- Section 7216 Frequently Asked Questions
- Bank Secrecy Act

Justice System Improvement Act of 1979

42 U.S.C. § 3701 et seq
42 U.S.C. § 3789(g) Confidentiality of information

Overview

As a Federal statistical agency that collects, analyzes, publishes, and disseminates a wide array of information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government, the Bureau of Justice Statistics (BJS) has taken aggressive measures to protect the privacy and confidentiality of individuals from whom they obtain information. BJS has procedures in place to ensure that information collected by BJS that is identifiable to a private person may only be used and/or revealed for the statistical or research-related purpose for which it is obtained. BJS has procedures in place to ensure that copies of such information shall not, without the consent of the person to whom the information pertains, be revealed to others who are not involved in the collection and analysis of the information.

Source

Bureau of Justice Statistics Data Quality Guidelines

Regulations

28 C.F.R. § 22

Supplemental Material

- BJS Data Protection Guidelines
- BJS Human Subjects/Confidentiality Requirements

National Security Act of 1947

50 U.S.C. § 3001 et seq
National Security Act of 1947

Overview

In the aftermath of World War II, the National Security Act provided a major reorganization of the U.S. defense and intelligence agencies. As amended, the Act provides “a comprehensive

program for the future security of the United States" through the integration of the policies and procedures of U.S. military, intelligence, and national security agencies, and the coordination of national security policy.

Source
National Security Act

Helpful Tips
Sec. 103D. Civil Liberties Protection Officer. (50 U.S.C. § 3029)

Executive Orders, Memoranda, and Directives
- United States Intelligence Activities, Exec. Order No. 12333, Fed. Reg. Vol. 46, No. 59941 (Dec. 04, 1981), amended by Exec. Order
- Further Strengthening the Sharing of Terrorism Information to Protect Americans, Exec. Order No. 13388, Fed. Reg. Vol. 70, No. 207 (Oct. 25, 2005)
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 2016)

Paperwork Reduction Act of 1995 (PRA)
44 U.S.C. Chapter 35 et seq

Overview
The Paperwork Reduction Act (PRA), signed into law in 1980 and reauthorized in 1995, provides the statutory framework for the Federal government's collection, use, and dissemination of information. The goals of the PRA include (1) minimizing paperwork and reporting burdens on the American public and (2) ensuring the maximum possible utility from the information that is collected.

In support of these goals, the PRA requires Federal agencies to take specific steps before requiring or requesting information from the public. These steps include (1) seeking public comment on proposed information collections and (2) submitting proposed collections for review and approval by the Office of Management and Budget (OMB). Within OMB, the Office of Information and Regulatory Affairs (OIRA) carries out the information collection review.

One of the purposes of the Paperwork Reduction Act is to "ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to (A) privacy and confidentiality, including section 552a of title 5; (B) security of information, including section 11332 of title 40; and (C) access to information, including section 552 of title 5." 44 U.S.C. § 3501(8).

Source
Office of Information and Regulatory Affairs – Regulations and the Rule Making Process

Helpful Tips
The Paperwork Reduction Act was signed into law in 1980, reauthorized in 1995, and subsequently amended.

Regulations
5 C.F.R. § 1320

Executive Orders, Memoranda, and Directives
Office of Management and Budget

- OMB Circular No. A-130, Managing Information as a Strategic Resource (July 2016)
- Flexibilities under the Paperwork Reduction Act for Compliance with Information Collection Requirements (July 2016)
- Behavioral Science Insights and Federal Forms (Sept. 2015)
- Web-based Interactive Technologies: Data Search Tools, Calculators, and the Paperwork Reduction Act (Sept. 2014)
- Testing and Simplifying Federal Forms (Aug. 2012)
- Reducing Reporting and Paperwork Burdens (June 2012)
- OMB Memorandum M-11-26, New Fast-Track Process for Collecting Service Delivery Feedback Under the Paperwork Reduction Act (June 2011)
- OMB Memorandum M-11-07, Facilitating Scientific Research by Streamlining the Paperwork Reduction Act Process (Dec. 2010)
- Paperwork Reduction Act – Generic Clearances (May 2010)
- Information Collection under the Paperwork Reduction Act (Apr. 2010)
- Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (Apr. 2010)
- Standards and Guidelines for Statistical Surveys (Sept. 2006)
- Guidance on Agency Survey and Statistical Information Collections (Jan. 2006)

Patient Safety and Quality Improvement Act of 2005 (PSQIA)
42 U.S.C. § 299b-21 – b-26
Patient Safety and Quality Improvement Act of 2005 (Public Law 109-41).

Overview
The Patient Safety and Quality Improvement Act of 2005 (PSQIA) establishes a voluntary reporting system designed to enhance the data available to assess and resolve patient safety and health care quality issues. To encourage the reporting and analysis of medical errors, PSQIA provides Federal privilege and confidentiality protections for patient safety information, called patient safety work product. PSQIA authorizes the U.S. Department of Health and Human

Services (HHS) to impose civil money penalties for violations of patient safety confidentiality. PSQIA also authorizes the Agency for Healthcare Research and Quality (AHRQ) to list patient safety organizations (PSOs). PSOs are the external experts that collect and review patient safety information.

Source
Health Information Privacy: Patient Safety and Quality Improvement Act of 2005 Statute and Rule

Helpful Tips
The PSQIA amends the Public Health Service Act (42 U.S.C. 299 et. seq.; Public Law No. 109-41) by inserting sections 921 through 926, 42 U.S.C. § 299b-21 through 299b-26. The Patient Safety Rule implements select provisions of PSQIA.

Subpart C of the Patient Safety Rule establishes the confidentiality provisions and disclosure permissions for patient safety work product and the enforcement procedures for violations of confidentiality pursuant to section 922 of the statute. The U.S. Department of Health and Human Services, Office for Civil Rights enforces these confidentiality protections.

AHRQ lists patient safety organizations pursuant to section 924 of PSQIA and has responsibility for common formats and network of patient safety databases pursuant to section 923.

Source
Health Information Privacy: Patient Safety and Quality Act of 2005

Regulations
42 C.F.R. Part 3

Statutory Implementation Guidance
U.S. Department of Health and Human Services
Office for Civil Rights
- HHS Guidance Regarding Patient Safety Work Product and Providers' External Obligations (May 2016)
- Guidance Regarding Patient Safety Organizations' Reporting Obligations to the FDA (December 2010)

Supplemental Material
U.S. Department of Health and Human Services
- Understanding Patient Safety Confidentiality
- Guidance for Patient Safety Rule

Privacy Act of 1974 (Privacy Act)

5 U.S.C. § 552a

Overview

The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires U.S. Government agencies give public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.

Source

U.S. Department of Justice – Privacy Act of 1974

Helpful Tips

The Computer Matching and Privacy Protection Act of 1988 (Pub. Law 100-503), amended the Privacy Act to include provisions governing computer-matching activities – those provisions have been incorporated into the Privacy Act.

Section 7 of Public Law 93-579, regarding Social Security numbers was originally part of the Privacy Act, but was not codified; it may be found at §552a in the note section. Similarly, Sections 6 and 9 of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, may also be found at §552a in the note section.

Statutory Implementation Guidance

Office of Management and Budget

- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 12, 2016)
- Computer Matching and Privacy Protection Amendments of 1990 and the Privacy Act of 1974) (56 FR 18599, April 23, 1991)
- Final guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988 (54 FR 25818, June 19, 1989)
- Guidance on Privacy Act Implications of “Call Detail” Programs (52 FR 12290, April 20, 1987)
- Implementation of the Privacy Act of 1974, Supplementary Guidance (40 FR 5674, November 21, 1975)

- Privacy Act Implementation, Guidelines and Responsibilities (OMB) (40 FR 28948, July 9, 1975)

Executive Orders, Memoranda, and Directives

- OMB Circular A-130, Managing Federal Information as a Strategic Resource (July 2016)
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 2016)
- OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (Dec. 2000)

OMB Memorandum for Privacy Act Officers of Departments and Agencies

- Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act (June 21, 2000)

OMB Memorandum for Agency Chief Information Officers

- Biennial Privacy Act and Computer Matching Reports (June 1998)

OMB Memorandum for the Chief Information Officers

- Privacy Act Responsibilities for Implementing the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (November 3, 1997)

OMB Memorandum for the Senior Agency Officials for Information Resources Management

- Privacy Act Guidance — Update (May 24, 1985)

OMB Memorandum M-83-11, Guidelines on the Relationship Between the Privacy Act of 1974 and the Debt Collection Act of 1982

- Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974 (April 11, 1983)

OMB Memorandum to the Heads of Executive Departments and Establishments

- Congressional Inquiries which Entail Access to Personal Information Subject to the Privacy Act (October 3, 1975)

Supplemental Material

Overview of the Privacy Act of 1974, U.S. Department of Justice

---

Protection of Pupil Rights Amendment (PPRA)

20 U.S.C. § 1232h

Overview

The PPRA applies to the programs and activities of a State educational agency (SEA), local educational agency (LEA), or other recipient of funds under any program funded by the U.S. Department of Education. It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

- political affiliations or beliefs of the student or the student's parent;
- mental or psychological problems of the student or the student's family;
- sex behavior or attitudes;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;
- legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- religious practices, affiliations, or beliefs of the student or student's parent; or,
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

PPRA also concerns marketing surveys and other areas of student privacy, parental access to information, and the administration of certain physical examinations to minors. The rights under PPRA transfer from the parents to a student who is 18 years old or an emancipated minor under State law.

Source

Family Policy Compliance Office: Protection of Pupil Rights Amendment (PPRA)

Helpful Tips

PPRA may also be known as Section 445 of the General Education Provisions Act.

Source

U.S. Department of Education: General Education Provisions Act

Regulations

34 C.F.R. Part 98

Supplemental Material

- Department of Education's Family Policy Compliance Office
- Department of Education's Privacy Technical Assistance Center
- Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices

---

Public Health Service Act (Certificates of Confidentiality)

42 U.S.C. Ch. 6A
42 U.S.C. § 241(d) Protection of privacy of individuals who are research subjects

Overview

Under section 301(d) of the Public Health Service Act (42 U.S.C. § 241(d)), the Secretary of the U.S. Department of Health and Human Services may authorize persons engaged in biomedical, behavioral, clinical, or other research to protect the privacy of individuals who are the subjects of that research. This authority has been delegated to the National Institutes of Health (NIH). Persons authorized by the NIH to protect the privacy of research subjects may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify them by name or other identifying characteristic.

Source

Certificates of Confidentiality Background

Public Health Service Act (Confidentiality of Health Statistics)

42 U.S.C. Ch. 6A

- See also: 42 U.S.C. § 242m(d)
- See also: Section 308(d) of the Public Health Service Act

Overview

The Public Health Service Act, 42 U.S.C. Ch. 6A, provision regarding the confidentiality of health statistics prohibits the National Center for Health Statistics (NCHS) from using any personal information for any purpose other than what was described to survey participants and from sharing that information with anyone not clearly mentioned to them. This provision enables NCHS to assure respondents strict confidentiality.

Source

How NCHS Protects Your Privacy

Supplemental Material

- How NCHS Protects Your Privacy: Confidentiality and Security of Information Collected by The National Center for Health Statistics
- NCHS Staff Manual on Confidentiality

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act)

Pub.L. 114-23, 129 Stat. 268

Overview

The ‘‘Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015’’ or the ‘‘USA FREEDOM Act of 2015’’ was enacted “to reform the authorities of the Federal Government to require the production of certain business records [e.g., call detail records], conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.”

Source

Pub.L. 114-23, 129 Stat. 268

Helpful Tips

The USA FREEDOM Act was enacted June 2, 2015, amending the Foreign Intelligence Surveillance Act of 1978 (FISA).

- TITLE I—FISA Business Records Reforms
- TITLE II— FISA Pen Register and Trap and Trace Device Reform
- TITLE III— FISA Acquisitions Targeting Persons outside the United States
- TITLE IV— Foreign Intelligence Court Reforms
- TITLE V— National Security Letter Reform
- TITLE VI— FISA Transparency and Reporting Requirements
- TITLE VII— Enhanced National Security Provisions
- TITLE VIII— Safety of Maritime Navigation and Nuclear Terrorism Conventions Implementation

Supplemental Material

Loretta E. Lynch, Attorney General of the United States

- “Minimization Procedures Used by the National Security Agency in connection with the Production of Call Detail Records Pursuant to Section 501 of the Foreign Intelligence Surveillance Act, as amended,” November 24, 2015

National Security Agency (NSA) Civil Liberties and Privacy Office

- Transparency Report: The USA FREEDOM Act Business Records FISA Implementation, January 15, 2016

Privacy and Civil Liberties Oversight Board (PCLOB)

- Recommendations Assessment Report, February 5, 2016

U.S. Department of Justice, Federal Bureau of Investigation (FBI)

- Termination Procedures for National Security Letter Nondisclosure Requirement, November 24, 2015

Director of the Administrative Office of the U.S. Courts

- Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2015

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)

Public Law 107-56

Overview

The USA PATRIOT Act was enacted in response to the attacks of September 11, 2001, and became law less than two months after those attacks. The Act comprises ten categories, called "titles."

- TITLE I—Enhancing Domestic Security against Terrorism
- TITLE II—Enhanced Surveillance Procedures
- TITLE III—International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001
- TITLE IV— Protecting the Border
- TITLE V— Removing Obstacles to Investigating Terrorism
- TITLE VI— Providing for Victims of Terrorism, Public Safety Officers, and their Families
- TITLE VII— Increased Information Sharing for Critical Infrastructure Protection
- TITLE VIII— Strengthening the Criminal Laws against Terrorism
- TITLE IX— Improved Intelligence
- TITLE X— Miscellaneous

Source

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001

Helpful Tips

The USA PATRIOT Act modified many major U.S. intelligence, communications, and privacy laws, including: The Electronic Communications Privacy Act (EPCA), which modifies Title III of the Omnibus Crime Control and Safe Streets Act (the Wiretap Act); the Foreign Intelligence Surveillance Act of 1978 (FISA); and the Communications Act of 1934. The USA PATRIOT Act has been reauthorized and amended several times since its initial enactment.

- The USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 The reauthorizing legislation made permanent 14 of the 16 sunsetted USA PATRIOT Act provisions and placed four-year sunsets on the other two—the authority to conduct "roving" surveillance under the Foreign Intelligence Surveillance Act (FISA) and the authority to request production of business records under FISA (USA PATRIOT Act sections 206 and 215, respectively).

Among the 14 USA PATRIOT Act provisions made permanent are:

- Facilitating enhanced information-sharing and coordination between national security and law enforcement personnel.
- Adding certain chemical weapons offenses, international terrorism, nuclear and weapons of mass destruction threats, and computer espionage offenses to the list of wiretap predicates.
- Allowing Internet Service Providers to disclose customer records voluntarily to the government in emergencies involving an immediate risk of death or serious physical injury.
- Permitting victims of computer trespass (hacking) crimes to request law enforcement assistance in monitoring trespassers on their computers.

Source

Fact Sheet: USA Patriot Act Improvement And Reauthorization Act of 2005 (Department of Justice)

- The USA PATRIOT Act Additional Reauthorization Amendments Act of 2006, Pub. L. No. 109-178, was written to clarify that individuals who receive FISA orders can challenge nondisclosure requirements; that individuals who receive national security letters are not required to disclose the name of their attorney; and that libraries are not wire or electronic communication service providers unless they provide specific services.

Source

S. 2271, 112th Congress, Second Session

- The PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, amended the USA PATRIOT Improvement and Reauthorization Act of 2005 to extend until June 1, 2015, provisions concerning roving electronic surveillance orders, requests for the production of business records and other tangible things; and amended the Intelligence Reform and Terrorism Prevention Act of 2004 to extend until June 1, 2015, a provision revising the definition of an “agent of a foreign power” to include any non-U.S. person who engages in international terrorism or preparatory activities (the “lone wolf” provision).

Source

Justice Information Sharing, USA PATRIOT Act

- On June 2, 2015, Congress passed and the President signed the USA FREEDOM Act of 2015, Pub. L. No. 114-23. The Act reauthorized several important national security authorities; banned bulk collection under Section 215 of the USA PATRIOT Act, under the pen register and trap and trace provisions found in Title IV of Foreign Intelligence Surveillance Act (FISA), or pursuant to National Security Letters; adopted the new legal mechanism proposed by the President regarding the targeted production of telephony metadata; made significant modifications to proceedings before the FISC; and built on the U.S. Government’s unprecedented transparency about intelligence activities.

Source
Transition to New Telephone Metadata Program (ODNI)

Executive Orders, Memoranda, and Directives

- United States Intelligence Activities, Exec. Order No. 12333 (46 FR 59941, Dec. 08, 1981), amended by Exec. Order 13284 (68 FR 4057, Jan. 28, 2003), Exec. Order 13355 (69 FR 53593, Sept. 1, 2004), and Exec. Order 13470 (73 FR 45325, Aug. 4, 2008)
- Further Strengthening the Sharing of Terrorism Information to Protect Americans, Exec. Order No. 13388 (70 FR 62023, Oct. 27, 2005)
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 2016)