SUMMARY OF SELECTED FEDERAL LAWS AND REGULATIONS ADDRESSING CONFIDENTIALITY, PRIVACY AND SECURITY

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
The Privacy Act of 1974	*5 U.S.C. § 552a; 45 C.F.R. Part 5b; OMB Circular No. A-108 (1975)*	The Privacy Act of 1974 is a withholding statute.	Any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency	The Privacy Act applies when the federal government maintains a system of records by which information about individuals is retrieved by use of the individuals' personal identifiers (names, social security numbers, or any other codes or identifiers that are assigned to the individual). A "record" for purposes of the Privacy Act means any item, collection, or grouping of information about an individual that is maintained by the agency and that contains the individual's name or other personal identifier.	The Privacy Act of 1974 and its implementing regulations: 1) Prohibits the disclosure of personally identifiable information maintained by agencies is a system of records without the consent of the subject individual, subject to twelve codified exceptions (2) Grants individuals increased rights of access to agency records maintained on themselves. (3) Grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete. (4) Establishes a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.
The Freedom of Information Act (FOIA) 5 U.S.C. § 552 (2006), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121Stat. 2524.	*5 U.S.C. § 552; 45 C.F.R. Part 5*	The Freedom of Information Act is a disclosure statute.	Agencies within the Executive Branch of the federal government, including independent regulatory agencies and some components within the Executive Office of the President, are subject to the provisions of the FOIA.	Records that are (1) either created or obtained by an agency, and (2) under agency control at the time of the FOIA request.	When an agency receives a proper FOIA request for records it must make the records "promptly available" unless the records or portions of the records are exempt from mandatory disclosure under subsection (b), or excluded under subsection (c). Subsection (b) of the FOIA establishes nine exemptions from disclosure, which were created by Congress to permit agencies to protect from disclosure certain specific types of information. Exemption 6 of subsection (b) allows for the withholding of personnel, medical, or similar files, the release of which would constitute a clearly unwarranted invasion of personal privacy. Exemption 7(C) provides protection for law enforcement information, the disclosure of which could reasonably be expected to constitute an unwarranted invasion of personal privacy. Subsection (c) of the FOIA establishes three special categories of law enforcement-related records that are entirely excluded from the coverage of the FOIA in order to

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
					safeguard against specific types of harm. The extraordinary protection embodied in subsection (c) permits an agency to respond to a request for such records as if the records in fact did not exist.
Health Insurance Portability and Accountability Act (HIPAA), Privacy Rule (2000)	*See generally, Pub. L. No. 104-191 (42 U.S.C. § 1320d-2 note)* *45 C.F.R. Part 160 and Subparts A and E of Part 164* *See generally http://www.hhs.gov/ocr/privacy/index.html*	Establishes national standards regarding health information privacy	Covered health entities; indirectly, business associates (who will become directly covered in 2010 pursuant to the American Recovery and Reinvestment Act of 2009)	Protected health information (certain individually identifiable health information)	Provides a federal floor of health information privacy protection; more protective state laws remain in force. The Rule assures certain individual rights in health information, imposes restrictions on uses and disclosures of protected health information, and provides for civil and criminal penalties for violations.
Health Insurance Portability and Accountability Act (HIPAA) Security Rule	*42 U.S.C. § 1320d-2(d)* *45 C.F.R. Part 160 and Subparts A and C of Part 164* *See Generally http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf*	Establishes national required and addressable security standards.	Covered health entities; indirectly business associates (who will become directly covered in 2010 pursuant to the American Recovery and Reinvestment Act of 2009)	Electronic protected health information (certain electronic individually identifiable information)	Works in tandem with HIPAA Privacy Rule and lays out three types of security safeguards required for compliance: administrative, physical, and technical.
Health Breach Notification Rule (Federal Trade Commission Rule)	*16 C.F.R. Part 318* *http://www.ftc.gov/os/2009/04/R911002healthbreach.pdf*	This proposed rule requires vendors of personal health records (PHRs) and related entities to notify individuals when their individually identifiable health information is breached	Vendors of PHRs, their related entities, and and other third party service providers who do not qualify as entities covered under HIPAA	Unsecured identifiable health information of an individual in a personal health record	These proposed rule requires vendors of personal health records (PHRs) and related entities to provide notice to consumers following a security breach. Stipulates that if a service provider of a PHR vendor experiences a breach, it must notify the PHR vendor. The PHR vendor, in turn, must notify consumers of the breach. The proposed rule contains additional requirements governing the standard for what triggers the notice, as well as the timing, method, and content of notice.

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
Health Breach Notification Rule (Health and Human Services)	45 C.F.R. Parts 160 and Subparts A and D of Part 164 *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf*	Requires notification from HIPAA covered entities, upon discovery of a breach of security	HIPAA covered entities; business associates	HIPAA protected health information	Requires covered entities to provide notice to patients, HHS, and in some cases, the media following a breach of unsecured protected health information. Aso requires business associates to notify covered entities following the discovery of such a breach.
SAMHSA: Confidentiality of Substance Abuse Patient Records	*42 U.S.C. § 290dd-2, 42 C.F.R. Part 2*	Confidentiality of substance abuse patient records (alcohol and drug abuse patient records)	Federally assisted alcohol and drug abuse programs that provide diagnosis, treatment or referral for treatment	Substance abuse patient records; information that identifies a person as an alcohol or drug abuser	It is prohibited to disclose substance abuse patient records and information that identifies an individual as an alcohol or drug abuser without obtaining the written consent of the individual. The regulations establish limited circumstances permitting disclosures without consent for medical emergencies, audit/evaluation activities, and research. Other disclosures without patient consent are permitted with an authorizing court order issued by a court of competent jurisdiction.
Medicaid Privacy Requirements	*42 U.S.C. 1396a(a)(7)* *42 C.F.R. §§ 431.300-307*	Administrative privacy requirements for Medicaid State agencies	States holding data related to Medicaid beneficiaries	Information concerning applicants for and recipients of Medicaid	A State plan must provide, under a State statute that imposes legal sanctions, safeguards meeting the requirements of this subpart that restrict the use or disclosure of information concerning Medicaid applicants and recipients to purposes directly connected with the administration of the plan and, at the option of the States, the exchange of information necessary to verify the certification of eligibility of children for free or reduced school meals.
Genetic Information Nondiscrimination Act of 2008 (GINA)	*Pub. L. No. 110-233* *http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/content-detail.html* HHS Office for Civil Rights Proposed Rule *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/ginanprm*	Protections for genetic information in health insurance and employment	Group health plans and employers (amends ERISA)	Genetic test results, family history, or use of genetic services in the individual or family members	Generally, prohibits discrimination by group health plans and employers on the basis of genetic information. Prohibits a group health plan from adjusting premium or contribution amounts for a group on the basis of genetic information, requesting or requiring an individual or family member to undergo a genetic test, or from using or disclosing genetic information for underwriting or enrollment determination. Allows plans to request but not require genetic testing for research. Prohibits employers from using genetic information for terminating, not hiring, refusing to include in special programs and training, or affecting employment status in any way. Requires genetic information held by employers to be maintained in separate files and prohibits disclosure of such information except under extremely limited circumstances. Agencies with regulatory authority include the Departments of Labor, Health and Human Services and Treasury.

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
	.pdf Equal Employment Opportunity Commission regulation 74 Fed. Reg. 9056 Proposed Rule *29 C.F.R. Part 1635* *http://edocket.access.gpo.gov/2009/E9-4221.htm* HHS, Labor, and Treasury Final Rule *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/ginaifr.pdf*				
Clinical Laboratory Improvement Amendments (CLIA) (1988)	*42 U.S.C. § 263a* *42 C.F.R. §493.1291* *http://wwwn.cdc.gov/clia/regs/toc.aspx*	Regulates laboratories conducting testing on human specimens for medical purposes	Any facility which performs laboratory testing on human specimens for medical purposes	Identifiable lab specimens and test results	Assures quality standards for all laboratory testing to ensure the accuracy, reliability and timeliness of patient test results. Certified labs may disclose test results or reports only to authorized people, those responsible for using (i.e. those treating the patient) the results, and the referring lab in a reference lab scenario; State laws define who is authorized, which may or may not include the patient.
Federal Food, Drug, and Cosmetic Act (FDCA)	21 U.S.C. § 301, *et.seq.* *See generally* 21 C.F.R. Part 50	Assures the safety of food and drug products	Any product or activity that falls within its jurisdiction	Confidential information that may identify human subjects	Generally, no investigator may involve a human being as a subject in research covered by these regulations unless the investigator has obtained the legally effective informed consent of the subject or the subject's legally authorized representative. An investigator must seek such consent only under circumstances that provide the prospective subject or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence. In seeking informed consent, a statement must be provided to the each subject describing the extent, if any, to which confidentiality of records

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
					identifying the subject will be maintained and that notes the possibility that the Food and Drug Administration may inspect the records.
Controlled Substances Act (CSA)	21 U.S.C. § 801, *et. seq.* *21 C.F.R. § 1316.23*	Allows researchers to petition the U.S. Attorney General for a grant of confidentiality to protect the identify of human subjects	Bona fide research projects directly related to the enforcement of the laws under the jurisdiction of the U.S. Attorney General	Identity of persons involved in research of drugs and substances covered under the Controlled Substances Act	Protects identifiable research information from forced or compelled disclosure. Allows for refusal to disclose identifying information regarding research participants in civil, criminal, administrative, legislative, or other proceedings
Federal Policy for the Protection of Human Subjects (Common Rule)	*45 C.F.R.* §§ *46.111(a)(7), 46.116(a)(5)* *http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm* *See* http://www.hhs.gov/ohrp/policy/common.html for codifications of the Common Rule into various agency regulations	Procedures and protections for human subjects participating in research funded by Federal agencies which adopted the Common Rule	Institutions, institutional review boards (IRBs), investigators conducting research	Research records identifying the subject and research data, which both can include health information	Governs Institutional Review Boards (IRBs) which exercise oversight of human subject research. As a prerequisite for IRB approval of research is that, when appropriate, the research must include adequate provisions protecting the privacy of subjects and maintaining confidentiality of data. Requires obtaining informed consent from research subjects, which includes providing subjects with information about the extent, if any, to which confidentiality of records identifying the subject will be maintained.
Statutory Authority for Certificates of Confidentiality	*42 U.S.C. 241(d)*	Allows the Secretary of HHS to issue a certificate to protect information from disclosure	Researchers	Identity of persons involved in biomedical, behavioral, clinical, or other research (including research on mental health, and on the use and effect of alcohol and other psychoactive drugs	Certificates of confidentiality may be Issued by the National Institutes of Health (NIH) and other HHS agencies to protect identifiable research information from forced or compelled disclosure. They allow for refusal to disclose identifying information on research participants in civil, criminal, administrative, legislative, or other proceedings.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
AHRQ Confidentiality Provisions	*42 U.S.C. §§ 299c-3(c), (d)*	Requires AHRQ to get consent from subjects or suppliers of data before releasing identifiable data	Identifiable data collected by AHRQ	Data collected for health care improvement research or patient safety research by AHRQ	Data collected by AHRQ cannot be used for any purpose other than the purpose for which it was supplied unless the identifiable establishment, person, or other supplier of the data has consented to its use for such other purpose. Provides a civil penalty of up to $10,000 for individuals who violate this provision.
CDC Confidentiality Provisions	*42 U.S.C. § 242m(d)*	Requires CDC to get consent before releasing identifiable information	Data collected by CDC	Data collected for research, evaluations, and demonstrations in health statistics, health services, and health care technology	Data collected by CDC cannot be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Secretary) to its use for such other purpose.
SAMHSA: Confidentiality Provisions for Data Collection and Survey Information	*42 U.S.C. § 290aa(n)*	Requires the consent of the person or establishment prior to use or release of identifiable information	Data obtained in the course of activities undertaken or supported by collected by SAMHSA	Data on mental health and substance abuse	Identifiable information obtained in the course of activities undertaken or supported by SAMHSA pursuant to data collection activities authorized under 42 U.S.C. §290aa-4 may not be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Secretary) to its use for such other purpose.
Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act)	*42 U.S.C. 299b-21 to 299b-26; 42 C.F.R. Part 3 http://edocket.access.gpo.gov/2008/E8-27475.htm*	Allows providers to voluntarily report information to Patient Safety Organizations (PSOs), on a privileged and confidential basis, for aggregation and analysis of patient safety events.	PSOs and providers that voluntarily participate	Data related to patient safety events	Establishes a framework by which hospitals, doctors, and other health care providers may voluntarily report information related to patient safety events (termed "patient safety work product") to Patient Safety Organizations (PSOs), on a privileged and confidential basis, for aggregation and analysis of patient safety events. Does not shield providers from having to comply with other Federal, state, or local laws pertaining to medical errors. PSO is a statutorily defined term of art and, by statute, the organizations must be listed by ARHQ, acting on behalf of the HHS Secretary.
Employee Retirement Income Security Act of 1974 (ERISA)	*29 U.S.C. § 1132*	Provision of consumer information by certain health plans	Private industry pension and health plans	Personal health information	Requires pension and health benefits plans to provide information about plan features and funding to consumers; provides fiduciary responsibilities for management and control of plan assets; establish a plan grievance and appeals process; and gives plan members the right to sue for benefits and breaches of fiduciary duty, including breaches of privacy.

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
					Responsibility for the interpretation and enforcement of ERISA is divided among the Department of Labor, the Department of the Treasury, and the Pension Benefit Guaranty Corporation.
Individuals with Disabilities Education Improvement Act (2004)	20 U.S.C. § 1400, *et seq.* 34 C.F.R. Parts 300 and 301 http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=81055712322+1+0+0&WAISaction=retrieve	Ensure services to children with disabilities	All public and private schools receiving federal funds	Educational records	Governs how states and public agencies provide early intervention, special education and related services to children with disabilities; infants, toddlers, children and youth with disabilities. Includes requirements regarding surrogate parents, notice and parental consent regarding disability information.
Family Educational Rights and Privacy Act (1974)	20 U.S.C. § 1232g 34 C.F.R. Part 99 http://www.ed.gov/policy/gen/reg/ferpa/index.html	Privacy of student education records	Educational agencies and institutions that receive funds under any program administered by the Secretary of Education	Educational records maintained by the institution that relate directly to the student	Limits disclosure of educational records maintained by agencies and institutions that receive federal funding. Protects the confidentiality of student records to some extent, while also giving students the right to review their own records. "Directory information" is not protected.
Protection of Pupil Rights Amendment (2002)	20 U.S.C. § 1232h 34 C.F.R. Part 98 http://www4.law.cornell.edu/uscode/20/1232h.html	Protects rights of parents and students	Programs with funding from the U.S. Department of Education	Personal information, including some health related information	Protects the rights of parents and students by 1) making instructional materials used in Department of Education funded surveys and analyses available to parents, and 2) ensuring that written parental consent is obtained before minor students participate in such surveys and analyses. Topics emphasized are: mental and psychological problems; sex behavior and attitudes; illegal, anti-social, self-incriminating and demeaning behavior; and income. Parents or students who believe their rights under PPRA may have been violated may file a complaint with the Department of Education.
Right to Financial Privacy Act (1978)	12 U.S.C. § 3401, *et seq.*	Protects the confidentiality of personal financial records	Federal agencies	Personal financial records	Protects the confidentiality of personal financial records by requiring that federal government agencies provide individuals with a notice and an opportunity to object before a bank or other specified institution can disclose personal financial information to a federal government agency.
Financial Modernization Act (Gramm-Leach-Bliley Act 1999) and Privacy of Consumer	15 U.S.C. §§ 6801-6809 16 C.F.R. Part 313	Protects non-public personal information collected by financial institutions	Any institution engaged in financial activities	Personal non-public information	Financial institutions must protect information collected about individuals; it does not apply to information collected in business or commercial activities. Financial institutions must issue privacy notices to their customers, with the opportunity to opt-out of some sharing of personally identifiable financial information with outside

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
Financial Information Regulations	http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr313_main_02.tpl				companies. Consumers have no right to stop sharing among affiliates, any company that controls, is controlled by, or is under common control with another company. Agencies with regulatory authority include the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission
Fair and Accurate Credit Transaction Act (FACTA) (2003)	Various provisions located throughout the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*	Combats identity theft and allows consumers to exercise greater control over their personal information Adds a new section 604(g)(1) to the Fair Credit Reporting Act	Credit reporting agencies	Consumer information	Allows consumers to request and obtain a free credit report once every twelve months; individuals can place alerts on their credit histories if identity theft is suspected, or if deploying overseas in the military to deter fraudulent credit applications; requires secure disposal of consumer information.
Fair Credit Reporting Act (FCRA) (1970)	15 U.S.C. § 1681, *et seq.*	Protects consumers from certain disclosures by consumer reporting agencies	Credit reporting agencies	Personal information	Provides important protections for credit reports, consumer investigatory reports, and employment background checks. Requires credit reporting agencies to protect the confidentiality, accuracy, and relevance of credit information. Establishes a framework of Fair Information Practices for personal information: rights of data quality (access and correct), data security, use limitations, requirements for data destruction, notice, user participation (consent), and accountability. FCRA was re-visited in the Fair and Accurate Credit Transactions Act of 2003 (FACTA).
Fair Credit Reporting Medical Information Regulations (2005)	12 C.F.R. Part 717 http://www.access.gpo.gov/nara/cfr/waisidx_06/12cfr717_06.html	Allows creditors to obtain or use consumer medical information for any credit eligibility determination	Credit reporting agencies	Personal information	A creditor may not obtain or use medical information in connection with any determination of a consumer's eligibility, or continued eligibility, for credit except as permitted by regulations or FACTA. Creditors can obtain or use medical information for credit eligibility determinations where necessary for legitimate purposes, and may permit affiliates to share medical information with each other without becoming consumer reporting agencies.
Fair Debt Collection Practices Act (Revised 2006)	15 U.S.C. § 1692	Addresses abusive debt collection practices	Debt collectors	Personal information	Promotes fair debt collection and provides consumers the right to dispute the accuracy of debt information. Creates guidelines under which debt collectors may conduct business, defines rights of consumers involved with debt collectors, and prescribes penalties and remedies for violations. The debt collector may only contact the debtor's through his/her attorney; if no attorney, then the collector may contact other people, but only to obtain an address, phone number, and work location. Collectors usually are prohibited from contacting such third parties more than once.
Children's Online Privacy Protection Act (1998)	15 U.S.C. S§ 6501–6506	Protects children's personal information	Commercial web sites and other	Personal information	Protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
and accompanying rule	16 C.F.R. Part 312 http://www.ftc.gov/os/1999/10/64fr59888.htm	online	online services directed at children under 13, or which collect users' age		
Cable Communications Policy Act (1984)	47 U.S.C. § 551	Cable service privacy	Cable service providers	Personally identifiable information	Generally, cable service providers must obtain consent from the subscriber before collecting or disclosing any personal information and provide a written notice of privacy practices annually.
Telephone Consumer Protection Act (1991)	47 U.S.C. § 227	Restricts the use of automated telephone systems for telemarketing	Any business that solicits consumers by phone or other electronic media (fax, voice messages, text messaging)	Personal information	Governs the conduct of telephone solicitations or telemarketing. Requires the Federal Communications Commission to promulgate rules to protect residential telephone subscribers' privacy rights. Established the do not call list for consumers to opt out of telemarketing calls.
Video Privacy Protection Act (1988)	18 U.S.C. § 2710	Prevents disclosure of personally identifiable records of video rentals or purchases by consumers	Video service providers	Personal information and video preferences	Prohibits disclosure of customer records without consumer consent. Requires destruction of personally identifiable customer information when no longer necessary.
Drivers Privacy Protection Act (1994)	18 U.S.C. § 2721	Limits disclosures of personal drivers license information	Departments of motor vehicles	Personal information	Release of information for official functions requires the express consent of the individual. There are, however, a large number of exceptions, and disclosure is permitted for agency functions, civil/judicial proceedings, etc.
REAL ID Act (2005)	H.R. 1268, 109 P.L. 13	Requires states to implement new requirements for drivers licenses and identification cards	State governments	Personal information	Imposes specific federal driver's license standards. The standards govern what information must be collected for and on the license, and in what format. Requires use of enhanced data collection, automation and security protections. States must meet requirements related to: • information and security features for the cards • proof of identity and U.S. legal status • verification of the source documents provided Also requires each state to share its motor vehicle database with all other states.
Employee Polygraph Protection Act (1988)	29 U.S.C §§ 2001-2009 29 C.F.R. Part 801 http://finduslaw.com/employee_polygraph_protection_epp_	Prevents employers from requiring lie detector tests for employees or job applicants, with certain exceptions	Employers	Personal information	Prevents employers from using lie detector tests, either for pre-employment screening or during the course of employment, with certain exemptions. Employers generally may not require any employee or job applicant to take a lie detector test, or discharge, discipline, or discriminate against an employee or job applicant for refusing to take a test.

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
	29 u s code chapter 22				
Federal Trade Commission Act (FTCA) (1914)	15 U.S.C. § 41, *et seq*.	Established the Federal Trade Commission (FTC) and its roles; governs consumer protection and business competition in the United States	Trade and commerce activities	Information related to any questionable business practices	Maintains a competitive marketplace for both consumers and businesses by policing anticompetitive practices. Monitors unfair and deceptive acts or practices including the Telemarketing Sales Rule, the Pay-Per-Call Rule and the Equal Credit Opportunity Act. The FTC has the authority to adopt trade regulation rules that define unfair or deceptive acts in particular industries.
Federal Information Security Management Act (FISMA) (2002)	44 U.S.C. § 3541(a)(1)(A)	Ensures that federal government information systems and information have security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction	Executive branch of the federal government and to outside entities acting on behalf of the federal government, including government contractors	Any. System risks are determined by classifying the types of information in it	Requires a mandatory set of IT system security processes that must be followed for all federal information systems. Compliance is monitored through yearly audits. As of 2008, annual reports must include: 1) by agency, the number of each type of privacy review conducted that year; 2) information about the privacy advice provided by the Senior Agency Official for Privacy; 3) the number of written complaints for each type of privacy issue allegation received, and 4) the number of complaints the agency referred to another agency
Electronic Signatures in Global and National Commerce Act (2000)	15 U.S.C. § 7001, *et seq.*	Guarantees the same legal validity for electronic contracts and signatures as for those executed by hand	Applies to any transaction relating to the conduct of business, consumer or commercial affairs between two or more persons	Any information contained in contracts; individual signatures	A contract or signature may not be denied legal effect, validity, or enforceability solely because it is in electronic form. Facilitates the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically. Consumers have the right to be aware of and consent to the use of an electronic record/signature. However, the legal effectiveness of the record may be affected by the lack of informed consent. Addresses retention of contracts and records.
Telecommunications Act (1996)	104 P.L. 104-104, 110 Stat. 56 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ104.104	Governs telecommunications licensure and activities	Telecommunications companies	Personal information	Requires telephone companies to give customers explicit notice of their right to control the use of their personal information and obtain express written, oral or electronic approval for its use. Certain provisions relate to prevention of unfair billing practices for information or services provided over toll-free telephone calls, privacy of consumer information, and a report on the use of advance telecommunications services for medical purposes.

Disclaimer: *This information was prepared as an educational resource and should not be relied on or construed as legal advice. Use of this table alone will not ensure compliance with applicable Federal and State law.*

Please contact ONC.Request@hhs.gov attention Jonathan Ishee/Privacy Law Table if you have any comments or suggestions related to this document.

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
Stored Communications Act	18 U.S.C. § 2701, et seq.	Prohibits unauthorized access of electronic communications	Everyone	Wire or electronic communications	Prohibits unauthorized access of electronic communications and provides civil and criminal remedies for violations, including a private right of action for aggrieved individuals. Also requires notice in the event of unauthorized access to a consumer's electronic records.
Electronic Communications Privacy Act (1986)	18 U.S.C §§ 2510-22, 2701-11, 3121-26.	Protections for electronic communications	Federal agencies	Privileged communications	Protects wire, oral, and electronic communications while in transit, and communication held in electronic storage. It sets requirements for search warrants under some circumstances that are more stringent than in other settings. It also prohibits the use of devices to record dialing, routing, addressing, and signaling information used in transmitting wire or electronic communications without a search warrant. Exceptions include: No protection for employee using employers equipment and it is not unlawful to capture info if at least one person in conversation knows about activities
The PATRIOT Act (2001)	109 P.L. 177 (2005 reauthorization) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ177.109.pdf	Expands the authority of US law enforcement agencies to fight terrorism in the United States and abroad.	Federal enforcement agencies	Restricts, reduces or eliminates many federal privacy law protections	Significantly increased the surveillance and investigative powers of law enforcement agencies in the United States to monitor private communications and access personal information for the purpose of locating terrorists and preventing terrorist acts. Amends a number of federal laws that contain privacy protections.
Foreign Intelligence Surveillance Act (FISA) (1978)	50 U.S.C. §§1801–1811, 1821–29, 1841–46, and 1861–62	Provides procedures for the surveillance and collection of foreign intelligence	Federal agencies	Personal information obtained without warrants or knowledge of the individual	Created a court which meets in secret, and approves or denies requests for search warrants. The 2001 Patriot Act included provisions to bypass the FISA Court and conduct surveillance without a warrant.
Privacy Protection Act (1980)	42 U.S.C. § 2000aa, *et seq.*	Requires law enforcement use of subpoenas or voluntary cooperation to obtain evidence from those engaged in First Amendment activities	Government officers and employees	Personal information and personal privacy	Protects journalists and publishers from being required to turn over to law enforcement any work product and documentary materials, including sources, before it is disseminated to the public.
Communications Assistance for Law Enforcement Act (1994)	47 U.S.C. § 1001, *et seq.*	Defines telecommunications carriers' duty to cooperate in intercepting	Telecommunications carriers and manufacturers of telecommunications equipment	Customer personal information	Telecommunications carriers must assist law enforcement in executing electronic surveillance pursuant to lawful authorization. Requires telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure the necessary surveillance capabilities. Preserves law enforcement's ability to conduct lawfully-authorized electronic

Federal Law	Citation	General Description	Applicability	Information Covered	Summary
		communications for law enforcement and other purposes			surveillance while preserving public safety and the public's right to privacy. Includes some privacy enhancements, such as raising the standard for government access to transactional data.
Confidential Information Protection and Statistical Efficiency Act of 2002	Pub. L. 107-347, 116 Stat. 2962 (44 U.S.C. 3501	Protects the confidentiality of identifiable information acquired by federal agencies	Government agencies	Data supplied by Individuals and organizations to federal agencies under a pledge of confidentiality for statistical purposes	Data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.
Computer Fraud and Abuse Act	18 U.S.C. §1030	Protects computers used in Federal government, certain financial institutions or computers used in interstate and foreign commerce	Federal government, financial institutions, computers used in interstate commerce	Information stored in computers of the federal government or certain financial institutions or computers used in interstate and foreign commerce	Protects computers used in Federal government, certain financial institutions or computers unused in interstate and foreign commerce from unauthorized access. Imposes fines and imprisonment for violations.
Federal Trade Commission Identify Theft Rule	16 C.F.R. Part 681 *See* http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf	Require individuals and entities to develop processes that detect identity theft.	Financial institutions and creditors with covered accounts	Information stored by Financial Institutions and Creditors with Covered Accounts	Requires financial Institutions and creditors with covered accounts to develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. The program must describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program.