Privacy Committee's

Federal Privacy Law Compendium

Version 1.0 (April 2003)

Stuart McKee, CIO
Department of Information Services, State of Washington
Chair, Privacy Committee

Lester Nakamura, Administrator
Information and Communications Services Division
State of Hawaii
Vice-Chair, Privacy Committee

Introduction

The enactment of HIPAA and the subsequent promulgation of the HIPAA Rules, including the Privacy Rule, demonstrated that federal laws can have a tremendous impact on state government information system operations and policies. To help states identify and assess federal laws that may have privacy implications for state information systems and policies, the NASCIO Privacy Committee has developed the Federal Privacy Law Compendium, Version 1.0. It is intended to serve as a resource for summaries of federal laws that may have an impact on the privacy of citizens' information that is entrusted to state government. The Federal Privacy Law Compendium provides a starting point for states in their assessment of whether the summarized federal privacy laws will impact state information system operations and/or policies. In the future, the Privacy Committee plans to add summaries of other federal privacy laws that could have an impact on state government information systems and policies.

The Federal Privacy Law Compendium summarizes ten federal laws that deal with the privacy of information and highlights instances of potential impact on state government. The federal privacy laws summarized in the Compendium are:

- The Children's Online Privacy Protection Act of 1998 *[15 USC §§6501-6506]*
- The Computer Fraud and Abuse Act of 1984 *[18 USC §1030]*
- The Computer Matching & Privacy Protection Act of 1988 & Amendments of 1990 *[5 USC §552a(a)(8)-(13), (e)(12), (o), (p), (q), (r) & (u)]*
- The Driver's Privacy Protection Act of 1994 *[18 USC §§2721-2725]*
- The Electronic Communications Privacy Act of 1986 *[18 USC §§2701-2711, §3121, §1367]*
- The Fair Credit Reporting Act of 1970 *[15 USC §§1681-1681v]*
- The Family Educational Rights and Privacy Act of 1974 *[20 USC §1232g]*
- The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 *[15 USC §§6801-6809]*
- The Health Insurance Portability and Accountability Act of 1996 *[Public Law 104-191]*
- The Privacy Act of 1974 *[5 USC §552a]*

Acknowledgments

NASCIO would like to express our gratitude to the Privacy Committee's Chair, Stuart McKee, CIO, Department of Information Services, State of Washington, and Vice Chair, Lester Nakamura, Administrator, Information and Communications Services Division, State of Hawaii, for the time, energy and guidance they generously contributed to this publication. NASCIO also thanks Roselyn Marcus, State of Washington, for lending her expertise to the review and revision of this publication. We would like to thank Richard Varn, former Privacy Committee Chair, for his vision for and contribution to this publication. Finally, NASCIO would like to extend many thanks to the following state editorial reviewers for their thoughtful comments and suggestions:

Scott Bream, State of Washington
Marty Daybell, State of Washington
Don Hildebrand, State of Maine
Renee Mauzy, State of Texas
Valerie McNevin, State of Colorado
Vanessa Mitra, State of Texas
Kym Patterson, State of Arkansas
Christy Ridout, State of Washington
Al Sherwood, State of Utah

Please direct any questions or comments about NASCIO's Federal Privacy Law Compendium to Mary Gay Whitmer, Issues Coordinator, at mwhitmer@amrinc.net or (859) 514-9209.

Table of Contents

The Children's Online Privacy Protection Act of 1998

Summary:

The Children's Online Privacy Protection Act (COPPA), 15 USC §§6501-6506, enacted in 1998, gave parents a way to control the information that is collected from their children online.[1] COPPA provided general requirements for website operators to follow and authorized the Federal Trade Commission (FTC) to promulgate regulations to clarify and implement its requirements. In 1999, the FTC passed its Final Rule on COPPA.[2]

Application and General Provisions: COPPA specifically applies to the operators of *commercial* websites and online services directed to children under 13 or that have actual knowledge that they are collecting personal information from children under 13. Personal information is information that is individually identifying including:

- A first and last name
- Home or physical address
- E-mail address
- Phone number
- Social Security Number
- Any other identifier determined by the FTC to permit the physical or online contacting of a specific individual
- Other information about the child or parent that the website collects online from the child and is combined with any of the above-described identifiers.

COPPA applies both to information collected directly and also indirectly from children through cookies or other tracking mechanisms.[3]

To control commercial websites' collection of children's personal information, COPPA:

- Requires notice of the collection, use and disclosure of children's personal information
- Requires verifiable parental consent for the collection, use and disclosure of children's personal information
- Allows parents a right to refuse to allow their children's personal information to be collected
- Prohibits the collection of more personal information than is reasonably necessary from a child in order for the child to participate in an on-line activity, such as a game
- Requires that operators establish reasonable procedures to protect the security, integrity and confidentiality of children's personal information.[4]

---

[1] Federal Trade Commission, "Statutes Relating To Consumer Protection Mission: The Children's Online Privacy Protection Act," September 13, 2001, <http://www.ftc.gov/ogc/stat3.htm>.
[2] 15 USC §6502(b)(1), <http://www4.law.cornell.edu/uscode/15/ch91.html> and 16 CFR Part 312, <http://www.ftc.gov/os/1999/9910/64fr59888.pdf>.
[3] 15 USC §6501 & 16 CFR §§312.2-312.3. See also, FTC, "How to Comply with the Children's Online Privacy Protection Rule," November 1999, <http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm>.
[4] 15 USC §6502(b)

The COPPA Final Rule: The Final Rule adds more detail to COPPA's general requirements. For example, website operators must provide a link on their websites to a notice of their information practices. The notices must contain the following information:

- The name, address, phone number and e-mail address of the website operator
- The types of personal information collected from children
- Whether children's personal information is collected directly or passively
- How the operator uses such information
- Whether children's personal information is disclosed to third parties (and, if so, other information about such third parties, including the type of business in which the third party is engaged and whether the third party has agreed to maintain the confidentiality, security and integrity of the personal information)
- A statement that the operator cannot condition a child's participation in an activity on the disclosure of more personal information than is reasonably necessary to participate in the activity
- A parent's right to agree to the collection of his or her child's information without agreeing to the disclosure of the information to third parties
- A parent's right to review and delete previously collected information
- A parent's right to refuse the further collection of his or her child's personal information.[5]

Exceptions: COPPA and its Final Rule provide limited exceptions that allow for the collection of children's personal information without parental consent. Exceptions are intended to cover certain children's activities, such as contests, newsletters, homework help and electronic postcards.[6] For example, website operators can collect children's personal information in order to issue a one-time response to a child's inquiry, for the sole purpose of obtaining parental consent or to provide information for law enforcement investigations.[7]

The COPPA Final Rule contains a "sliding scale" provision that allows website operators to use other methods of obtaining parental consent if the child's personal information will not be disclosed to third parties.[8] However, the method used must be reasonable to verify parental consent given the use of the information. For instance, a website operator who only uses a child's personal information for internal purposes can use e-mail to obtain parental consent (as long as the operator takes additional steps to ensure that the parent is the party granting consent). On the other hand, to disclose a child's personal information to a third party, an operator must use a more reliable consent verification method, such as the collection of a parent's credit card number or a digital signature. The Final Rule specified that this provision would end or "sunset" in April 2002 because of the technological advances in electronic verification methods.[9] However, in April 2002, the FTC chose to extend the "sliding scale" provision until April

[5] 16 CFR §312.4
[6] FTC, "How to Comply with the Children's Online Privacy Protection Rule," November 1999
[7] 15 USC §6502(b)(2) & 16 CFR §312.5(c)
[8] 16 CFR §312.5 (a)-(b) & FTC, "How to Comply with the Children's Online Privacy Protection Rule," November 1999
[9] 16 CFR §312.5(b)

21, 2005, because the public comments submitted to the FTC "indicated that secure electronic technology and infomediary services are not yet widely available at a reasonable cost and that the sliding scale mechanism to date has been an effective method for obtaining parental consent."[10]

COPPA and its Final Rule also provide industry groups with the opportunity to establish FTC-approved self-regulatory guidelines that, if followed, will provide a "safe harbor" for operators within those industries, meaning that such operators will be deemed by the FTC to be in compliance with COPPA, if they follow such FTC-approved guidelines.[11]

Finally, not later than five years after the regulation's effective date, the FTC must review and report to Congress.[12]

Relevance for State Government:

COPPA and its Final Rule apply to commercial website operators. They do not appear to directly apply to federal or state government websites. However, in a June 22, 2000 Office of Management and Budget (OMB) Memorandum, OMB directed all federal agencies and all contractors, when operating on behalf of federal agencies, to comply with the requirements of COPPA for federal "web sites directed to children."[13] At their discretion, states may also choose to incorporate components of COPPA in their own privacy policies.

In addition to enforcement at the federal level, COPPA may also be enforced at the state level. COPPA allows a state attorney general to bring a civil action if a commercial website operator violates COPPA and there is reason to believe that an interest of the state has been or is currently being threatened or adversely affected. Before filing such an action, a state attorney general must give notice of the lawsuit to the FTC. The FTC has a right to intervene in state COPPA enforcement actions.[14] However, state and local governments may not impose liability on website operators engaging in interstate or foreign commerce in a way that is inconsistent with COPPA and its Final Rule.[15]

View the Text of COPPA at: http://www4.law.cornell.edu/uscode/15/ch91.html

View the Text of the COPPA Final Rule at:
http://www.ftc.gov/os/1999/9910/64fr59888.pdf (including explanatory discussion of differences between the FTC's Proposed Rule and the Final Rule)

View the OMB Memorandum Requiring Federal Agencies' Compliance with COPPA at:

---

[10] FTC, "FTC Protecting Children's Privacy Online," April 22, 2002, <http://www.ftc.gov/opa/2002/04/coppaanniv.htm>.
[11] 15 USC §6503 & 16 CFR §312.10.
[12] 15 USC §6506
[13] Office of Management and Budget, Memorandum, Privacy Policies and Data Collection on Federal Web Sites, M-00-13, June 22, 2000, <http://www.whitehouse.gov/omb/memoranda/m00-13.html>.
[14] 15 USC §6504
[15] 15 USC §6502(d)

http://www.whitehouse.gov/omb/memoranda/m00-13.html

View Summaries of COPPA at:

Privacilla: http://www.privacilla.org/business/online/coppa.html

FTC: http://www.ftc.gov/ogc/stat3.htm

View a FTC Guide on "How to Comply with the Children's Online Privacy Protection Rule" at: http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm

The Computer Fraud and Abuse Act

Summary:

The Computer Fraud and Abuse Act of 1984 (CFAA), 18 U.S.C. §1030, created in the advent of increased computer hacking in the 1980's, made illegal the unauthorized access to US government computers.[16] Through amendments in 1986, 1994 and 1996, CFAA was broadened to protect computers used in interstate commerce and to prohibit trafficking in computer passwords.[17] CFAA makes it illegal to access certain computers, such as US government computers and computers used in interstate commerce, and to access a computer without authorization to gain sensitive information, such as national defense or foreign relations information.[18] It also prohibits the furtherance of fraud through unauthorized access to computers engaged in interstate commerce. [19]

Additionally, CFAA makes it illegal to damage a "protected computer" by accessing it without authorization or transmitting a program, information or code to it.[20] A "protected computer" is a computer used by or for a financial institution or the US government or which is used in interstate commerce or foreign communications.[21] Because many state computers are used in interstate commerce, CFAA, as amended, may be broad enough to protect many state computer systems. The USA Patriot Act expanded the definition of a protected computer to include computers physically located outside of the US that affect "interstate or foreign commerce or communication of the United States."[22]

Unauthorized Access: CFAA makes the following types of unauthorized access to a computer illegal:

- Knowingly accessing a computer without authorization and gaining protected information, such as information regarding national defense or foreign relations, with reason to believe that the information could be used to injure the United States or give an advantage to a foreign nation, and communicating or attempting to communicate such information or willfully keeping the information from a person entitled to receive the information
- Intentionally accessing a computer without authorization and obtaining financial information from a financial institution or from a US government agency or department or information contained in the file of a consumer reporting agency

---

[16] Jones Telecommunications & Mutlimedia Encyclopedia, "Computer Fraud", July 9, 2001, available upon subscription at <http://www.digitalcentury.com/update/comfraud.html>.
[17] Note that Public Law 107-273 §4002(b)(1) & (12)(A)-(B) and §4005 (a)(3) & (d)(3) made clerical and other technical amendments to CFAA.
[18] 18 USC §1030(a)(1)-(2)
[19] 18 USC §1030(a)(4)
[20] 18 USC §1030(a)(5)
[21] 18 USC §1030(e)(2)
[22] Public Law 107-56 §814. View 18 USC §1030 as amended by Public Law 107-56 at <http://www.cdt.org/security/usapatriot/keyprovisions.pdf>.

- Intentionally accessing a computer without authorization and obtaining information from a protected computer, if the conduct affects interstate commerce or foreign communications
- Intentionally accessing a US government agency or department computer
- Knowingly and with the intent to defraud, accessing a protected computer and obtaining anything of value.[23]

Damaging a Protected Computer: CFAA criminalized the following:

- Knowingly transmitting a program, information, code or command and intentionally damaging a protected computer
- Intentionally accessing, without authorization, a protected computer and thereby recklessly damaging it
- Intentionally accessing, without authorization, a protected computer and causing damage to the computer.[24]

For these activities to violate CFAA, they must result in one of the following:

- Damage in the amount of $5,000 or more during a one-year period
- Modification or impairment (or the potential modification or impairment) of medical treatment or care
- Physical injury
- A threat to public health or safety, or
- Damage to a government computer system used in the administration of justice or national defense or security.[25]

The USA Patriot Act clarified that violators do not have to intend to cause $5,000 worth of damage, but need only intend to impair data, program, system or information integrity or availability. It allows the aggregation of monetary losses "from a related course of conduct affecting one or more other protected computers" from a one-year period to meet the $5,000 loss threshold.[26]

Password Trafficking & Other Criminal Activities: To combat the piracy of government computer passwords, CFAA criminalizes intentionally trafficking in computer passwords with the intent to defraud, where such trafficking affects interstate commerce or foreign relations or where the computer that may be accessed is a US government computer.[27] Under CFAA, it is also a crime to extort from persons or entities, including educational institutions and governmental entities, something of value by sending a threat to damage a protected computer through interstate communications or foreign commerce.[28] Finally, CFAA criminalizes attempts to violate its provisions.[29]

---

[23] 18 USC §1030(a)(1)-(4)
[24] 18 USC §1030(a)(5), as amended by Public Law 107-56 §814
[25] Ibid.
[26] US Department of Justice, Field Guidance on New Authorities (Redacted) as Enacted in the 2001 Anti-Terrorism Legislation, as provided by epic.org at <http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf>.
[27] 18 USC §1030(a)(6)
[28] 18 USC §1030(a)(7) & (e)(12), as amended by Public Law 107-56 §814
[29] 18 USC §1030(b)

Criminal Penalties: CFAA generally provides for criminal fines and jail sentences for violation of its provisions. Where there are repeat violations of CFAA, the criminal penalties may be increased.[30] Moreover, for those who damage a protected computer by the transmission of a program, information, code or command, the USA Patriot Act increased the maximum prison sentence from five years to ten years for first-time offenders and, for repeat offenders, from ten to twenty years.[31]

A Private Right of Action: CFAA provides for a private right of action for individuals who suffer damage or loss due to a CFAA violation. Aggrieved individuals may seek compensatory damages and injunctive relief.[32] However, the USA Patriot Act amended CFAA's private right of action provision to qualify that a civil action based upon a CFAA violation may only be brought if the violation involves one of the following factors:

- Causes damage of $5,000 or more within a one-year period
- Results in the modification or impairment (or the potential modification or impairment) of medical treatment or care
- Results in physical injury
- Causes a threat to public health or safety, or
- Damages a government computer system used in the administration of justice, national defense or security.[33]

Other Changes Made by the USA Patriot Act:

- Added the violation of CFAA as a predicate offense for obtaining a wireptap order to intercept wire communications[34]
- Allows law enforcement to intercept the communications of "computer trespassers," which includes those who access "protected computers" without authorization as defined by CFAA, but excludes those that the computer owner knows he has a contractual relationship with that permits access to the protected computer[35]
- Added as an offense damaging a protected computer used by or for a government entity for the administration of justice or national defense or security, even if the damage caused does not exceed $5,000
- Allows previous state law felonies for unauthorized access to a computer to trigger CFAA's provision that doubles maximum penalties for repeat offenders[36]

[30] 18 USC §1030(c)
[31] 18 USC §1030(c)(4)(A)-(C), as amended by Public Law 107-56 §814
[32] 18 USC §1030(g)
[33] 18 USC §1030(g), as amended by Public Law 107-56 §814
[34] Public Law 107-56 §202
[35] Public Law 107-56 §217. See also US Department of Justice, Field Guidance on New Authorities (Redacted) as Enacted in the 2001 Anti-Terrorism Legislation, as provided by epic.org.
[36] Public Law 107-56 §814. US Department of Justice, Field Guidance on New Authorities (Redacted) as Enacted in the 2001 Anti-Terrorism Legislation, as provided by epic.org.

- Added serious computer crimes to the definition of what may constitute a terrorist offense.[37]

Relevance to State Government:

CFAA was intended to only address federal and interstate computer crimes and does not appear to infringe on states' rights and/or computer laws.[38] CFAA specifically does not restrict state or local law enforcement from conducting investigative, protective or intelligence activities.[39] However, under certain circumstances, CFAA may provide some protection for state government computer systems, since many state computer systems are used in interstate commerce. The extortion provision of CFAA also covers those who extort "governmental entities," which includes state governments.

View the Legislative Summary at:

http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04718:|TOM:/bss/d099query.html|

View the Text of CFAA at:

http://www4.law.cornell.edu/uscode/18/1030.html

View the USA Patriot Act at:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

View the Redlined Text of CFAA as amended by the USA Patriot Act as provided by the Center for Democracy and Technology at:
http://www.cdt.org/security/usapatriot/keyprovisions.pdf

View a Summary of the USA Patriot Act at:
http://www.cybercrime.gov/PatriotAct.htm

Related Links:

General Privacy Law Materials at findlaw.com:
http://profs.lp.findlaw.com/privacy/index.html

US Department of Justice Cybercrime Materials:
http://www.usdoj.gov/criminal/cybercrime/1030_anal.html

[37] Public Law 107-56 §808
[38] Jones Telecommunications & Mutlimedia Encyclopedia, "Computer Fraud," July 9, 2001.
[39] 18 USC §1030(f).

The Computer Matching and Privacy Protection Act of 1988 and Amendments of 1990

Summary:

The Computer Matching and Privacy Protection Act of 1988[40] and the Computer Matching and Privacy Protection Amendments of 1990[41] (collectively referred to herein as "the Act") both amended the Privacy Act of 1974 to provide requirements federal agencies must follow when matching information on individuals with information held by other federal, state or local agencies.[42]

Computer Matching Agreements: A federal agency can only match information in its records with that of another agency if it enters into a written agreement with the other agency. Such written computer matching agreements must include detailed information about the computer matching activities. The agreements must include:

- The program's purpose and anticipated results
- The legal authority and justification for the matching program
- A description of the records to be matched
- A prohibition on the re-disclosure of a federal agency's records by the agency receiving the records, unless required by law or essential to conducting the computer matching program.

Computer matching agreements also must provide a detailed account of how the information will be handled by the agencies and how individuals will be notified that their information may be verified through a matching program.[43]

The agreements then are sent to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives. The agreements only remain in effect for a maximum of 18 months. They can be renewed for an additional one-year if the program will be conducted without any change and each agency certifies that it has been in compliance with the agreement.[44]

Data Integrity Boards: The Act requires every federal agency conducting or participating in a matching program to establish a data integrity board to oversee and coordinate the implementation of a computer matching program. Each board consists of senior officials designated by the agency head and the agency inspector general, if any. The board's duties, include:

- Approving computer-matching agreements
- Assessing compliance with the agreements
- Submitting an annual report to the agency head and the Office of Management and Budget.

---

[40] 5 USC §552a(a)(8)-(13), (e)(12), (o), (p), (q), (r) & (u), <http://www4.law.cornell.edu/uscode/5/552a.html>.
[41] 5 USC §552a(p)
[42] US Department of Justice, "Overview of the Privacy Act of 1974: Computer Matching," May 2000, <http://www.usdoj.gov/04foia/1974compmatch.htm>.
[43] 5 USC §552a(o)
[44] Ibid.

A data integrity board may only approve a computer-matching agreement if the program is likely to be cost-effective under a cost-benefit analysis. However, the board may waive this requirement in writing in accordance with the guidelines of the Office of Management and Budget, if it determines that a cost-benefit analysis is not required. Moreover, if a computer-matching program is statutorily required, then a cost-benefit analysis is not required.[45]

Determinations Based on Adverse Information: To protect against adverse effects on an individual from a computer matching program, the Act prohibits agencies, including state and local agencies, from denying, terminating or suspending financial assistance under a federal benefits program or taking any other action that is adverse to an individual without ensuring the integrity of the program's information. An agency must independently verify adverse information or wait for the federal agency's data integrity board to determine that (1) the information is limited to the identification and amount of benefits paid and (2) there is a high degree of confidence regarding the information's accuracy. Additionally, before taking any such adverse action, agencies must make sure that they meet the following notice requirements: (1) the individual must have received notice from the agency and had an opportunity to contest such findings and (2) the time period for an individual to respond must have expired.[46]

Relevance for State Government:

In order to participate in a computer matching program with a federal agency, state agencies must enter into a written agreement with a federal agency. The federal agency's data integrity board must monitor the state agency's compliance. State agencies involved in computer matching programs must not deny, suspend or terminate assistance under a federal program based upon information obtained through the computer matching program until the Act's notice requirements are met and the information can be independently verified or the federal agency's data integrity board makes a determination regarding the information's integrity.

View the Computer Matching and Privacy Protection Act of 1988 and 1990 Amendments as contained in the Privacy Act of 1974 at:
http://www4.law.cornell.edu/uscode/5/552a.html

View the Public Law Summary of:

The Computer Matching and Privacy Protection Act of 1988 at:
http://thomas.loc.gov/cgi-bin/bdquery/z?d100:SN00496:@@@L|TOM:/bss/d100query.html|

The Computer Matching and Privacy Protection Amendments of 1990 at:
http://thomas.loc.gov/cgi-bin/bdquery/z?d101:HR05835:@@@D&summ2=1&. See summary under Title VII, Subtitle C.

[45] 5 USC §522a(u)
[46] 5 USC §552a(p)(1)

View a Summary of the Computer Matching and Privacy Protection Act at Privacilla.org: http://www.privacilla.org/government/cmppa.html

View a Department of Justice Summary of the Act at:
http://www.usdoj.gov/04foia/1974compmatch.htm

The Driver's Privacy Protection Act of 1994

Summary:

The Driver's Privacy Protection Act (DPPA), 18 USC §§ 2721-2725, restricts disclosure of personal information obtained by state departments of motor vehicles (DMVs) in connection with a motor vehicle record. A motor vehicle record is defined as "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles."[47] The DPPA specifies when and how state DMVs may disclose such information. In 1994, Congress enacted the DPPA in response to actress Rebecca Shaeffer's murder. Tragically, the killer obtained her address from the California Department of Motor Vehicles.[48]

Types of Protected Information: The DPPA classifies certain information possessed by state DMVs as "personal information." The DPPA prohibits disclosure of this information, unless it falls under one of the DPPA's fourteen enumerated exceptions. Personal information "means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."[49] In October 2000, an amendment to the DPPA established a second category of "highly restricted personal information" and gave it extra protection against disclosure. This new category of personal information includes an individual's photo or image, social security number, and medical or disability information. "Highly restricted personal information" cannot be disclosed without the "express consent of the person to whom such information applies." Only four of the DPPA's exceptions can be applied to disclose "highly restricted personal information" without an individual's express consent.[50] Note that "express consent" means that an individual's consent must be in writing or conveyed electronically so that it bears an electronic signature.[51]

Other Protections of the DPPA: In addition to prohibiting the disclosure of "personal information" and "highly restricted personal information," the DPPA explicitly prohibits states from conditioning or burdening the issuance of a motor vehicle record in order to obtain an individual's consent to divulge such information. However, this does not prohibit state DMVs from charging an administrative fee in connection with the issuance of a motor vehicle record.[52] Individuals who knowingly violate the DPPA shall be criminally fined and subject to a civil action for damages, including punitive damages, in U.S. District Court. Moreover, if a state DMV has a policy or practice that results in

---

[47] 18 USC §2725(1)
[48] Privacilla.org, "The Drivers Privacy Protection Act," December 20, 2000, <http://privacilla.org/government/dppahistory.html>.
[49] 18 USC §2721(a)-(b) & §2725(3), <http://www.accessreports.com/statutes/DPPA1.htm>.
[50] 18 USC §2721(a)(2) & §2725(4), <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ346.106.pdf> at §309.
[51] 18 USC §2725(5)
[52] 18 USC §2721(e)

"substantial noncompliance," the Attorney General shall impose a civil penalty of not more than $5,000 per day for each day of substantial noncompliance.[53]

The Exceptions: In addition to the DPPA's fourteen enumerated exceptions, information can be disclosed to carry out the purposes of a number of other laws, including the Clean Air Act, the Anti Car Theft Act of 1992, and the Automobile Information Disclosure Act. The DPPA's enumerated exceptions allow the disclosure of "personal information" in the following situations:

- For use by any government agency in carrying out its functions
- For use in matters of motor vehicle safety or driver safety and theft
- In connection with legal proceedings
- For use in research activities and statistical reports
- For use by insurers in underwriting and claims investigations
- To provide notice to the owner of an impounded or towed vehicle
- To licensed private investigators or licensed security services
- To employers to verify information about the holder of a commercial license
- For use in the operation of private toll transportation facilities
- When a state DMV has obtained an individual's written consent.[54]

Other businesses also can obtain "personal information" from state DMVs "for use in the normal course of business." Businesses requesting such information must be "legitimate" and only may use the personal information to verify the accuracy of personal information submitted by an individual and, if the submitted information is incorrect, to obtain the correct information but only "for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual." With the express consent of an individual, state DMVs can disclose personal information for bulk distribution for surveys, marketing or solicitations. Finally, the DPPA generally permits the recipients of "personal information" to resell or redisclose such information, but only for the purposes specified in the DPPA's exceptions.[55]

"Highly restricted personal information" may only be disclosed without an individual's express consent in the following situations:

- For use by any government agency in carrying out its functions
- In connection with legal proceedings
- For use by insurers in underwriting and claims investigations
- For use by employers to verify information about the holder of a commercial license.[56]

Relevance for State Government:

This federal legislation directly applies to the states. Non-compliance may result in fines as well as civil actions by individuals whose information has been disclosed in violation of the DPPA. States, at their discretion, can enact their own versions of privacy

[53] 18 USC §2723 & §2724
[54] 18 USC §2721(b)
[55] 18 USC §2721(b)-(c)
[56] 18 USC §2721(a)(2)

protections to fill in any gaps. For example, the State of Utah has legislation that provides additional protections for personal information contained in motor vehicle title and registration records.[57] Note that the 2000 amendments have limited the application of most of the DPPA's exceptions when "highly restricted personal information," such as social security numbers, is involved.

View a Summary of the DPPA at:
http://privacilla.org/government/dppahistory.html

View the Original DPPA Provisions at:
http://www.accessreports.com/statutes/DPPA1.htm

View the 2000 DPPA Amendment at:

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ346.106

View the Current DPPA Statute with Amendments at:
http://www4.law.cornell.edu/uscode/18/pIch123.html

[57] See Utah Code Sections 41-1a-116, <http://www.le.state.ut.us/~code/TITLE41/htm/41_01017.htm> and 53-3-109, <http://www.le.state.ut.us/~code/TITLE53/htm/53_03009.htm>.

Electronic Communications Privacy Act of 1986

Summary:

Before the enactment of the Electronic Communications Privacy Act of 1986 (ECPA) only wire and oral communications were legally protected against unauthorized interception.[58] ECPA amended the federal wiretap statute to extend protection to specific types of electronic communications, such as e-mail, radio-paging devices, cell phones, private communications carriers, and computer transmissions.[59] It also extended the prohibition on interception to the communications of wire or electronic communication services. Prior to ECPA's enactment, only the communications of common carriers were covered.[60]

ECPA also added provisions that deal with access to stored wire and electronic communications and transaction records. This summary focuses on ECPA's access provisions. Note that the USA Patriot Act, Public Law 107-56, which was enacted in response to the September 11, 2001 terrorist attacks, made substantial changes to ECPA's interception and access provisions. This summary points out important aspects of these changes.[61]

Prohibitions on Access to Information: ECPA sets out prohibitions concerning access to stored wire and electronic communications and transactional records. It criminalizes intentionally accessing, without authorization, a facility that provides electronic communications services and obtaining, altering or preventing access to wire or electronic communications that are electronically stored in such a facility. Such violations are considered to be Class B misdemeanors with a penalty of imprisonment for not more than six months and a fine under Title 18. If the offense is committed to gain a commercial advantage, to cause malicious destruction or damage or for private commercial gain, then the penalty increases to a Class A misdemeanor with a possible prison sentence of not more than one year and a fine under Title 18. However, certain exceptions apply where the provider or user of the communications service authorizes access or where governmental entities are authorized to access such information under other legal provisions.[62]

Restrictions on the Disclosure of the Contents of Communications: ECPA prohibits electronic communication service providers and remote computing services[63] from disclosing the contents of communications that providers store, carry or maintain.

---

[58] Public Law 99-508, <http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04952:@@@L|TOM:/bss/d099query.html|>.
[59] Jones Telecommunications & Multimedia Encyclopedia, "Electronic Communications Privacy Act," July 9, 2001, available upon subscription at <http://www.digitalcentury.com/update/ecpa.html>.
[60] Public Law 99-508
[61] View a redlined version of statutes, including ECPA, that were amended by the USA Patriot Act at <http://www.cdt.org/security/010911response.shtml>.
[62] 18 USC §2701
[63] 18 USC §2711(2) defines a "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system."

However, there are certain exceptions under which a provider may disclose the contents of a communication, including:

- To the addressee or intended recipient of a communication
- With the consent of the communication's originator, addressee or intended recipient or the subscriber of a remote communications service
- To law enforcement where the provider inadvertently obtains the contents and the contents appears to relate to the commission of a crime.[64]

The USA Patriot Act added that a provider may disclose the contents of a communication where the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."[65]

Restrictions on the Disclosure of Customer Records and Information: The USA Patriot Act added a provision that prohibits remote computing services or electronic communications services from knowingly divulging customer or subscriber records or other information pertaining to a customer or subscriber (not including the contents of communications) to the government.[66] However, if a governmental entity meets any of the following exceptions, an electronic communications provider or a remote computing service must disclose a customer or subscriber record:

- Obtains a warrant
- Obtains a court order
- Obtains the consent of the subscriber or customer
- Obtains a formal written request relevant to a law enforcement investigation concerning telemarketing fraud.[67]

However, ECPA allows communications providers to disclose such customer information (not including the contents of communications) to persons other than governmental entities. Instances in which customer information may be divulged by a communications provider include as otherwise authorized in §2703, §2517 and §2511, with the customer's consent, and as necessary to render services to the customer or to protect the provider's rights or property.[68]

Required Disclosure to Governmental Entities of Customers' Stored Wire and Electronic Communications and Information: Electronic communications providers and remote computing services must disclose a customer's stored wire or electronic communications and information to a governmental entity as long as the governmental entity satisfies the requirements provided by ECPA. Note that, prior to the USA Patriot Act, for stored wire communications, such as voicemail messages, the federal wiretap statute required that law enforcement obtain a wiretap order for access. However, the USA Patriot Act amended ECPA to take the governance of access to stored wire communications out of the federal wiretap statute and place it under the provisions governing access to stored electronic communications (18 USC §2701-11). Now, law

[64] 18 USC §2702
[65] 18 USC §2702 as amended by Public Law 107-56 §212
[66] 18 USC §2702 as amended by Public Law 107-56 §212(a)
[67] 18 USC §2703(c) as amended by Public Law 107-56 §212(b) and §220(a)
[68] 18 USC §2702 as amended by Public Law 107-56 §212

enforcement must only obtain a search warrant to gain access to stored wire communications, which is a less burdensome process than obtaining a wiretap order.[69]

For access to the *contents* of a stored wire or electronic communication from an electronic communications service, government entities must obtain a federal or equivalent state search warrant, if the information has been stored by the provider for 180 days or less. If the wire or electronic information has been stored for more than 180 days or if the service provider is a "remote computing service," then the governmental entity must obtain a federal or state search warrant, a court order, or an administrative, grand jury or trial subpoena. The governmental entity must provide the subscriber or customer with notice of the disclosure unless access is gained pursuant to a search warrant.

Generally, electronic communication providers and remote computing services also must disclose customer or subscriber records to a governmental entity, if the governmental entity obtains a federal or state search warrant, court order, subscriber or customer consent or submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud. Notice to the customer or subscriber is not required when requesting such subscriber or customer information or records of communications.[70]

The USA Patriot Act amended ECPA to require that electronic communication providers and remote computing systems disclose an expanded list of information about a customer as long as a governmental entity obtains a federal or state search warrant, a court order, or a federal or state administrative, grand jury or trial subpoena. Prior to the USA Patriot Act's enactment, only a customer's name, address, local and long distance telephone toll billing records, phone number, and length of service could be disclosed. The USA Patriot Act added that such disclosures may include the type of service utilized, records of session times and duration, temporarily assigned network addresses, and the means and sources of payment, including credit card numbers and bank accounts. Note that a governmental entity does not have to provide notice to a customer or subscriber of its receipt of such records.[71]

Other Provisions of ECPA:

- Back-Up Copies of Requested Information: Governmental entities can request as part of a subpoena or court order that providers make back-up copies of the information requested.[72]
- Delay in Customer Notice: Governmental entities may apply to the court for an order allowing a delay in notifying a customer or subscriber of the court order granting access to the contents of communications where there is reason to believe that notification may have an adverse result.[73]

---

[69] Public Law 107-56 §209. See also US Department of Justice, Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation, <http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf>.

[70] 18 USC §2703, as amended by Public Law 107-56

[71] Ibid. See also US Department of Justice, Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation.

[72] 18 USC §2704

[73] 18 USC §2705

- Reimbursement for Providers: Providers can receive reimbursement for the cost of disclosing information to governmental entities.[74]
- Civil Liability: Civil lawsuits for damages, including punitive damages, can be brought where ECPA's provisions are willfully or intentionally violated (but note two exceptions, civil suits cannot be brought against the United States[75] or against communications providers for divulging information pursuant to a court order, warrant, subpoena or certification).[76] If a court determines that any agency of the United States has willfully or intentionally violated ECPA, the agency must initiate a proceeding to determine whether disciplinary action is warranted against an agency official or employee.[77]
- Disclosures for Counterintelligence: Wire or electronic service providers must comply with written requests from the FBI Director or his designee for disclosure of subscriber information, toll billing records, and transactional records for counterintelligence, and service providers are prohibited from disclosing the fact of such requests.[78]
- Videotape Service Providers: Videotape service providers can be held liable for knowingly disclosing personally identifiable customer information unless disclosure falls under certain exceptions, such as consumer consent or a law enforcement warrant.[79]
- Pen Registers and Trap and Trace Devices: The use of a pen register or a trap and tracing device is illegal without a court order. However, exceptions do apply in instances where a service provider must use pen registers or trap and tracing devices in its operations. The use of such devices also is permitted to record the fact of a wire or electronic communication or to protect a user from abusive use of the service. Criminal sanctions can be imposed for violating this section.[80] The USA Patriot Act amended the pen register and trap and trace device provisions of ECPA in a number of ways, including (1) allowing law enforcement to use pen registers and trap and trace devices on the Internet and computer networks and (2) allowing court orders for pen registers and trap and trace devices to have a nationwide effect.[81]
- Interference with Satellite Transmissions: Intentionally or maliciously interfering with a satellite transmission is prohibited and can result in a fine as well as up to ten years in prison. However, this prohibition does not apply to the investigative, protective or intelligence activities of a law enforcement agency or an intelligence agency of the United States.[82]

[74] 18 USC §2706
[75] 18 USC §2707
[76] 18 USC §2703(e)
[77] 18 USC §2707(d)
[78] 18 USC §2709
[79] 18 USC §2710
[80] 18 USC §3121, as amended by Public Law 107-56
[81] US Department of Justice, Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation
[82] 18 USC §1367

Relevance for State Government:

ECPA is relevant for governmental entities attempting to access the contents or records of wire or electronic communications. They must follow ECPA's requirements as well as adhere to ECPA's restrictions. The portion of ECPA dealing with restrictions on videotape rental and sales records pre-empts state and local laws dealing with the same subject only to the extent that state and local laws require disclosures prohibited by ECPA.

View a Legislative Summary of ECPA at:

http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04952:@@@L|TOM:/bss/d099query.html|

View the Text of ECPA at:

http://www4.law.cornell.edu/uscode/18/pIch119.html (18 USC §2510-2522)(federal wiretap statute)

http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/121/toc.html (18 USC §2701-2711)(stored electronic and communications access)

http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=3121 (18 USC §3121)(pen register and trap and trace devices)

http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=1367 (18 USC §1367)(interference with satellite transmissions)

View the Text of the USA Patriot Act at:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

View a Red-Lined Version of ECPA as Amended by the USA Patriot Act (from the Center for Democracy and Technology) at:

http://www.cdt.org/security/010911response.shtml

The Fair Credit Reporting Act of 1970

Summary:

The Fair Credit Reporting Act (FCRA), 15 USC §1681-§1681v,[83] recognizes the importance of fair and accurate credit information to the banking system and the public's confidence in the banking system. The purpose of FCRA is to ensure that consumer reporting agencies exercise their responsibility to adopt reasonable procedures to meet commercial needs in a manner that is fair and equitable to consumers in regard to confidentiality, accuracy and privacy. FCRA details the information that consumer credit reports may contain and how and by whom a consumer's credit information can be used.[84] The Federal Trade Commission (FTC) is the primary enforcement agency of FCRA.[85]

Permissible Uses of Consumer Credit Reports:

Generally: FCRA specifies the circumstances under which a consumer reporting agency can furnish a consumer report. A person can only obtain a consumer report for the purposes listed in the FCRA statute and must certify that purpose to the credit reporting agency before obtaining the report. Permissible uses include:

- Responding to a court order or subpoena
- Complying with the consumer's written instructions
- Extending credit or reviewing or collecting an account
- Employment purposes
- Underwriting insurance regarding the consumer
- Assessing the credit risk of a current credit obligation, and
- Other legitimate business needs in connection with a transaction initiated by the consumer or to determine if a consumer continues to meet the terms of his or her account with the user of a consumer report.[86]

Of Interest to State Government: FCRA also includes a number of uses that may be applicable to state government. FCRA specifically provides that a consumer reporting agency can give a government agency a consumer's name, address, former address, and current and former places of employment.[87] Other uses of interest to state government include:

- Determining a consumer's eligibility for a governmental license or benefit where the government agency is legally required to consider a consumer's financial status or responsibility
- Child support enforcement by a state or local agency, and
- Setting or modifying child support by an agency administering a state plan under the Social Security Act.[88]

---

[83] View the Fair Credit Reporting Act at <http://www.ftc.gov/os/statutes/fcrajan2002.pdf>.
[84] 15 USC §1681
[85] 15 USC §1681s
[86] 15 USC §1681b
[87] 15 USC §1681f
[88] 15 USC §1681b

Resale Procedures: To ensure that the proper use of consumer reports is maintained through the downstream resale of consumer reports, FCRA requires that resellers of consumer reports or any information contained therein disclose to the consumer reporting agency the identity of the end-user of the report or information and each permissible purpose for which the report or information will be used. Resellers of consumer reports also must have in place reasonable procedures for ensuring the identity and purpose of those to whom the reports are resold.[89]

Requirements for Certain Uses of Consumer Credit Information:

Employment Purposes: For certain uses, such as for employment purposes, FCRA provides requirements that the user of the information must fulfill. More specifically, for use in employing, promoting, reassigning or retaining an employee, an employer or prospective employer generally must:

- Disclose in writing to the employee or prospective employee the fact that a consumer report may be obtained
- Obtain the written authorization of the employee or prospective employee for the procurement of the report, and
- Certify to the consumer reporting agency that the appropriate disclosures have been made to the employee or prospective employee and that the information used in the report will not be used to violate federal or state equal employment opportunity laws or regulations.

The consumer reporting agency also must provide a summary of the consumer's rights under FCRA along with the report.[90]

Moreover, if adverse action is taken against the consumer by an employer or prospective employer based in whole or in part on information contained in a consumer report, the employer or prospective employer must provide the consumer with the following:

- A copy of the report, and
- A written description of the consumer's rights under FCRA. [91]

Other Types of Transactions: For other types of transactions, such as credit or insurance transactions that are not initiated by the consumer, consumer reporting agencies and the users of such information must comply with specific requirements. For example, a consumer reporting agency can disclose certain consumer credit information, such as name and address, if it maintains a system through which consumers can elect not to have their information disclosed.[92] Finally, a consumer's consent is required in order for a

[89] 15 USC §1681e(e)
[90] 15 USC §1681b
[91] 15 USC §1681b. Note that, for positions over which the Secretary of Transportation has authority to establish qualifications and maximum hours of service (or positions subject to safety regulation by a state transportation agency) and where the only contact with the consumer has been by phone, mail or electronic means, then this section of FCRA requires that an employer provide the consumer against whom adverse action was taken based in whole or in part on a consumer report with the following additional information: (1) that adverse action has been taken based in whole or in part on a consumer report, (2) the contact information of the consumer reporting agency, (3) that the consumer reporting agency did not make the adverse decision, and (4) that the consumer can obtain a free copy of the report and dispute the accuracy or completeness of the report with the consumer reporting agency.
[92] 15 USC §1681b & §1681m

consumer reporting agency to disclose medical information contained in a consumer report for employment purposes or in credit or insurance transactions.[93]

Requirements Where Adverse Action is Taken Against a Consumer:

FCRA places certain responsibilities on the users of consumer reports when they take adverse action against a consumer based in whole or in part on information contained in a report. In such situations, users must notify the consumer of the following by oral, written or electronic means:

- Notice of the adverse action
- The contact information of the consumer reporting agency
- Statement that the consumer reporting agency did not take the adverse action and cannot provide specific reasons why the action was taken, and
- Notice of the consumer's right to receive a free copy of the report upon request within 60 days and the consumer's right to dispute the accuracy or completeness of the information contained in the report.

In addition to employment situations, FCRA also provides for consumer notice requirements in situations where adverse action is taken against a consumer based upon information that is not directly obtained from a consumer reporting agency. For example, FCRA provides for consumer notice when adverse action has been taken against the consumer based on information from an affiliate that bears on a consumer's credit, reputation, personal characteristics or mode of living. FCRA also provides for consumer notice requirements when a person obtains information from a third party (other than a consumer reporting agency) regarding a consumer's credit, reputation, personal characteristics or mode of living, and then denies the consumer credit for personal, family or household purposes.[94]

Requirements Regarding the Content of Information in Consumer Reports:

FCRA places time limitations on certain types of information in consumer reports. For example, the following types of information cannot be included in a consumer reporting agency's report:

- Information of bankruptcy adjudications made more than 10 years before the consumer report
- Information about civil suits or judgments and records of arrest that were entered more than 7 years before the consumer report or have a statute of limitations which has expired, which ever is longer, and
- Information concerning paid tax liens, accounts placed for collection or charged to profit or loss, or other adverse items of information (other than records of criminal conviction) that are more than 7 years older than the consumer report.

However, for credit and insurance transactions with a principal or face amount of $150,000 or more and employment purposes regarding a position with an expected annual salary of $75,000 or more, the time restrictions listed above do not apply.

Consumer reporting agencies are required to indicate on consumer reports any accounts that were voluntarily closed by the consumer. In addition, if a consumer

[93] 15 USC §1681b
[94] 15 USC §1681m

disputes information in the consumer report, the report should indicate the disputed information.[95]

Requirements for Consumer Reporting Agencies:

Consumer reporting agencies must have in place reasonable procedures to ensure compliance with FCRA's requirements regarding information that must be included or excluded from consumer reports, the identity and purpose of consumer report users, and the accuracy of the information contained in the reports. FCRA also contains many measures to protect consumers as well as users of consumer reports. For example, consumer reporting agencies are barred from prohibiting the disclosure of consumer reports to consumers where the user of a report takes adverse action based on the report. Consumer reporting agencies also must disclose to any person who obtains a consumer report or any person who regularly, in the ordinary course of business, provides consumer information to the consumer reporting agency, a notice of such person's responsibilities under FCRA.[96]

Other important FCRA provisions for consumer reporting agencies include:

- Disclosure measures to protect consumers' credit reporting rights, including the duty of the consumer reporting agency to disclose, upon request, all information in a consumer's file and sources of information (excluding credit scores and risk scores or predictors)[97]
- Reinvestigation procedures to assist consumers who dispute the accuracy of information contained in their consumer reports,[98]and
- A price cap of $8.00 on the fee that a consumer reporting agency may charge consumers in providing them with consumer report information (some exceptions to the charges apply in cases of a consumer's financial hardship).[99]

Responsibilities of Furnishers of Information:

General Duties: FCRA has provisions that task the furnishers of consumer information to consumer reporting agencies with the duty to provide accurate information to the consumer reporting agencies. FCRA specifically prohibits anyone from furnishing consumer information to a consumer reporting agency if the person "knows or consciously avoids knowing that the information is inaccurate." However, liability for such violations can be avoided by the furnishers of consumer credit information, if they "clearly and conspicuously" specify to the consumer an address for reporting notices of inaccuracies.

The furnishers of information also are prohibited from supplying consumer information, if the consumer has notified the furnisher that the information is inaccurate, and the information, in fact, turns out to be inaccurate.

Other duties of the furnishers of consumer credit information include:

- Promptly notifying a consumer reporting agency of any previously furnished information that the furnisher has found to be inaccurate or incomplete

[95] 15 USC §1681c
[96] 15 USC §1681e
[97] 15 USC §1681g
[98] 15 USC §1681i
[99] 15 USC§1681j

- Furnishing a notice that particular information is disputed
- Providing a notice of accounts that have been closed by the consumer, and
- Providing a notice of delinquency of accounts.[100]

These duties are enforced through the power of federal and state officials to bring lawsuits to enjoin violations and to recover damages for which the furnisher would be liable to residents of the state if the residents of the state could bring suit for damages.[101]

Investigation of Inaccuracies: After a furnisher of information is notified of a dispute concerning the accuracy or completeness of information provided to a consumer reporting agency, the furnisher must conduct an investigation, reviewing all the relevant information provided by the consumer reporting agency. Upon the completion of the investigation, the furnisher must provide the consumer reporting agency with the results of the investigation. If the investigation reveals any inaccuracies or instances of incomplete information, then the furnisher must report the results to all other nationwide consumer reporting agencies to which the furnisher provided the information.[102]

Investigative Reports:

FCRA provides restrictions on investigative consumer reports, which are consumer reports that contain information "on a consumer's character, general reputation, personal characteristics, or mode of living" that is obtained through interviewing a consumer's neighbors, friends or associates.[103]

Duties of Persons Requesting an Investigative Report: To obtain an investigative report, a person must (1) disclose in writing to the consumer that such a report may be made, (2) include a notice of the consumer's right to obtain additional information and a summary of the consumer's FCRA rights, and (3) must certify compliance with FCRA's consumer disclosure and notice requirements described above as well as certify compliance with the disclosure of the nature and scope of the investigation if requested in writing by the consumer. However, by having reasonable compliance procedures in place, a person may avoid liability for any failures to satisfy these requirements.

Duties of Consumer Reporting Agencies in Compiling Investigative Reports: Consumer reporting agencies cannot compile an investigative report unless the person asking for the report has certified that he or she has made the consumer disclosures required by FCRA. To ensure the accuracy of information in investigative reports, consumer reporting agencies also must verify any public record information relating to an arrest, indictment, conviction, civil action, tax lien or outstanding judgment within a thirty-day period before furnishing the report. In addition, consumer reporting agencies generally must follow reasonable procedures to verify adverse information obtained from a consumer's neighbors, friends or associates[104] and cannot use adverse information (other than public record information) from an investigative report in subsequent consumer reports unless the information is verified in the process of making the subsequent report or was received within three months of the furnishing of the subsequent report.[105]

---

[100] 15 USC §1681s-2
[101] 15 USC §1681s-2 & §1681s
[102] 15 USC §1681s-2
[103] 15 USC §1681a
[104] 15 USC §1681d
[105] 15 USC §1681l

Civil and Criminal Liability:

Civil Liability: Generally, persons, including corporations and governmental entities,[106] willfully failing to comply with FCRA will be liable to the consumer for actual damages sustained in an amount not less than $100 and not more than $1,000 plus any punitive damages allowed by the court, court costs, and reasonable attorney's fees. However, where the violation is committed by a natural person who obtains a consumer report under false pretenses or knowingly obtains a consumer report without a permissible purpose, a person can be liable for the greater of $1,000 or the amount of actual damages, in addition to any punitive damages, court costs and reasonable attorney's fees. Persons (again including corporations and governmental entities) also may be held liable to a consumer reporting agency for obtaining a consumer report under false pretenses or knowingly without a permissible purpose for the greater of $1,000 or the amount of actual damages sustained by the consumer reporting agency.[107] Finally, consumers may recover actual damages, court costs and reasonable attorney's fees as determined by the court from persons negligently violating FCRA's requirements.[108]

Criminal Liability: The following violations may result in criminal penalties in the form of fines under Title 18 of the United States Code or not more than two years in jail or both:[109]

- Where a person knowingly and willfully obtains information about a consumer from a consumer reporting agency under false pretenses [110] or
- Where an officer or employee of a consumer reporting agency knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive such information.[111]

Enforcement:

Generally: FCRA is enforced by the Federal Trade Commission under the Federal Trade Commission Act, except to the extent that enforcement is specifically committed to another agency. For entities specified in FCRA, such as banks and air carriers, other federal laws are used to enforce FCRA, including the Federal Deposit Insurance Act and the Federal Aviation Act.[112]

State Enforcement Rights: States may bring actions to enjoin violations of FCRA. States also may bring actions to recover damages on behalf of its residents for:

- Willful or negligent noncompliance with FCRA, and
- Violation of FCRA's requirements for furnishers of information.[113]

States also can recover court costs and reasonable attorney's fees.[114]

However, due to the involvement of the FTC in enforcing FCRA's provisions, states must provide notice to the FTC or appropriate federal regulator before filing an

---

[106] 15 USC §1681a(b)
[107] 15 USC §1681n
[108] 15 USC §1681o
[109] 15 USC §1681q & §1681r
[110] 15 USC §1681q
[111] 15 USC §1681r
[112] 15 USC §1681s
[113] An action for damages may only be brought if a person has violated an injunction that prohibits violations of FCRA.
[114] 15 USC §1681s

action under FCRA. The FTC or other appropriate federal regulator also has the right to intervene, to be heard on all matters, to remove the case to U.S. District Court and to file petitions for appeal. However, when there is a federal action pending for a violation of FCRA, then a state may not bring an action under FCRA against any defendant named in the federal lawsuit's complaint.[115]

Relation to State Law:

FCRA does not affect consistent state laws dealing with the collection, distribution or use of consumer information. Inconsistent state laws are only affected by FCRA to the extent of their inconsistency. However, exceptions exist that prevent states from regulating certain areas covered by FCRA, including the prescreening of consumer reports. Note, however, that such exceptions do not apply to state laws that (1) are enacted after January 1, 2004, (2) explicitly state the intent to supplement FCRA, and (3) provide greater consumer protection than FCRA.[116]

Disclosures to the FBI for Counterintelligence Purposes and Governmental Agencies for Counterterrorism Purposes:

FCRA provides for the disclosure to the FBI for counterintelligence purposes of the names and addresses of all financial institutions at which a consumer has an account. The FBI must submit requests for such information in writing for investigations to protect against international terrorism or clandestine intelligence activities. The USA Patriot Act, enacted in response to the September 11, 2001 terrorist attacks, revised this portion of FCRA to allow for FBI officials lower down in the chain of command to determine in writing that the information is sought for international terrorism purposes or clandestine intelligence activities.[117] The USA Patriot Act also revised FCRA to allow a consumer reporting agency to furnish consumer reports to a government agency that is authorized to conduct investigations or intelligence or counterintelligence related to international terrorism. A government agency must certify this in writing.[118]

Relevance for State Government:

Although the intent of FCRA is to provide for better consumer protections and more accurate consumer credit information, FCRA's requirements do impact state government for a number of reasons. First, under certain circumstances, state government entities can use information from consumer credit reporting agencies. Secondly, states maintain public record information that is used by credit reporting agencies. States also have authority to bring suits to enforce FCRA on behalf of state residents. Finally, consistent state laws dealing with consumer credit reporting generally remain intact, while inconsistent state laws are trumped by FCRA to the extent of their inconsistency.

[115] Ibid.
[116] 15 USC §1681t
[117] 15 USC §1681u
[118] 15 USC §1681v

View the Text of FCRA at:
http://www.ftc.gov/os/statutes/fcrajan2002.pdf

View a Summary of Consumer FCRA Rights at:
http://www.pueblo.gsa.gov/cic_text/money/fair-credit/fair-crd.htm

Family Educational Rights and Privacy Act of 1974 (FERPA)

Summary:

The Family Educational Rights and Privacy Act (FERPA), 20 USC §1232g,[119] provides privacy protection for students' education records, while ensuring a parent's rights to access his or her child's education records, correct mistakes in those records, and know who has requested or obtained the records.

Application of FERPA: FERPA applies to an educational agency or institution, which is considered any public or private agency or institution that receives funds under any of the US Department of Education's applicable programs.[120] An applicable program is any program for which the Secretary of Education or the Department of Education has an administrative responsibility under the law.[121]

Transfer of Rights Under FERPA: The rights afforded to a student's parents under FERPA are transferred to the student when the student turns 18 or if the student is attending a postsecondary educational institution.[122]

Records Subject to FERPA: Education records covered by FERPA are records that contain information directly related to a student and are maintained by an educational agency or institution or a person acting for an educational agency or institution. Education records NOT covered by FERPA include records:

- Of educational personnel, such as teachers, and other school personnel where the records are in the sole possession of such personnel and are not accessible or revealed to anyone else except a substitute
- Maintained by an educational agency or institution's law enforcement unit
- Of employees of the educational agency or institution who are not in attendance at such agency or institution and who made and maintained such records in the normal course of business and where such records are not available for use for any other purpose
- Medical records, including psychiatric records, for a student who is 18 years of age or older and attending a postsecondary institution, which were made during a student's treatment and are not accessible to anyone other than those treating the student.[123]

Parents' Review and Inspection Rights: Under FERPA, educational agencies and institutions can be denied funds under any applicable program, where they deny or

---

[119] View 20 USC §1232g at: <http://www4.law.cornell.edu/uscode/20/1232g.html>. Note that Public Law 107-110 §1062 made several technical corrections to FERPA that are grammatical in nature. View PL 107-110 at: <http://thomas.loc.gov/>.
[120] 20 USC §1232g(a)(3)
[121] 20 USC §1221(c)(1), <http://www4.law.cornell.edu/uscode/20/1221.html>.
[122] 20 USC §1232g(d)
[123] 20 USC §1232g(a)(4)

effectively prevent a student's parents from inspecting and reviewing the student's educational records. Educational agencies and institutions must establish procedures for granting such requests for parental access within not more than forty-five days from the date the request is made.[124]

The right to review and inspect education records under FERPA also applies specifically to state educational agencies and institutions regardless of whether or not they are considered an educational agency or institution under FERPA's other provisions. FERPA provides that such state educational agencies and institutions can be denied funds under an applicable program where they have a policy of denying or effectively prevent a parent from inspecting his or her child's education records maintained by that state agency or institution for children who are or have been in attendance at any school of an educational agency or institution that is subject to FERPA.[125]

Records that are exempted from a parent's right of inspection and review include: (1) parents' financial records or information (2) and confidential letters and statements of recommendation, if placed in the student's file prior to January 1, 1975.[126]

For confidential recommendations, such as for admission to a school or for an application for employment, a student may waive his or her right of access as long as (1) upon a student's request, the student is provided with the names of all persons making confidential recommendations (2) the recommendations are used solely for their intended purpose and (3) a waiver is not required as a condition to admission to school or receipt of financial aid or other services or benefits.[127]

Opportunity to Correct Inaccurate Records: Educational agencies and institutions also can be denied funds if a student's parent is not afforded an opportunity for a hearing regarding information in his or her child's records that may be inaccurate, misleading or otherwise in violation of the student's privacy rights. A parent must have the opportunity to correct or delete such information. Finally, a parent has the right to insert into a student's record a written explanation with respect to the content of the student's records.[128]

Student's Directory Information: Information that is considered "directory information" may be made publicly accessible as long as an educational agency or institution gives public notice of the categories of information to be made public and allows parents a reasonable time period to inform the agency or institution that the parent must give consent before such information is released. "Directory information" includes a student's name, address, telephone number, date and place of birth, major, participation in school activities or sports, weight and height for students on athletic teams, dates of attendance, degrees, awards, and the most recent educational institution previously attended by a student.[129]

---

[124] 20 USC §1232g(a)(1)(A)
[125] 20 USC §1232g(a)(1)(B)
[126] 20 USC §1232g(a)(1)(C)
[127] 20 USC §1232g(a)(1)(D)
[128] 20 USC §1232g(a)(2)
[129] 20 USC §1232g(a)(5)

Release of Education Records: Educational agencies and institutions also may be denied funds if they have a policy or practice of releasing students' education records or personally identifiable information therein (with the exception of students' directory information) without a parent's written consent. FERPA contains many exceptions that allow for the release of education records and personally identifiable information, such as:

To School Officials including:

- School officials of the student's school, including teachers, who have a legitimate educational interest, including the student's educational interest
- School officials of an institution in which a student wants to enroll provided that the school (1) notify parents of the transfer of records (2) allow the parents to obtain a copy of the records, if requested, and (3) allow a hearing for any challenges to the content of the records
- Representatives of the Comptroller of the US, the Secretary of Education, state educational authorities for audit purposes, and authorized representatives of the Attorney General for law enforcement purposes

For Administrative Purposes including:

- In connection with the application or receipt of financial aid
- School studies for predictive tests, student aid or improving instruction
- Accrediting functions of accrediting organizations

For Law Enforcement or Judicial Purposes including:

- To state and local officials under a state statute allowing the reporting or disclosure where the reporting or disclosure concerns the juvenile justice system and would allow that system to better serve the juvenile (Note: Where such statutes were enacted after November 19, 1974, officials to whom the information is disclosed must certify in writing that they will not disclose the information except with written parental consent unless permitted by a state law.)
- Where ordered by a subpoena for law enforcement purposes or in connection with grand jury proceedings

Other:

- To the parents of a dependent child
- In emergency situations, subject to the Secretary's regulations, where the information is necessary for the student's or another person's health or safety.[130]

Restrictions on Access to Students' Personally Identifiable Information: Under FERPA, educational agencies and institutions can be denied funds where there is a policy or practice of releasing or providing access to students' personally identifiable

[130] 20 USC §1232g(b)(1)

information where it is not otherwise permitted by statute. Again, note that a student's directory information can be disclosed as long as the disclosure is in keeping with FERPA's other requirements regarding that information. Exceptions include the written consent of the parent and compliance with a judicial order or subpoena.[131]

Another notable exception allows state educational authorities to access student records where it is necessary for the audit or evaluation of a federally supported educational program or for the enforcement of other federal legal requirements related to such programs. Additionally, except where the collection of personally identifiable information is authorized by federal law, students' personally identifiable information must be protected from disclosure by officials using it under this exception. The information also must be destroyed once those officials no longer need it.[132]

Requirements Regarding Records on Access and Disclosure: FERPA requires that educational agencies and institutions maintain records of who has requested or obtained access to a student's education records. The records must indicate the legitimate interest of persons who have obtained the information. The records of access are only available to parents, school officials who are the custodians of such records, other school officials with legitimate educational interests, and others in connection with auditing the operation of the system.[133]

Restrictions on Third Parties Who Obtain a Student's Personally Identifiable Information: A student's personally identifiable information only can be transferred to a third party under FERPA with the restriction that the third party will not permit access to anyone else without written parental consent. If a third party outside of the educational agency or institution violates this restriction or fails to destroy the information after its use in a study, then the agency or institution must not allow that person access for a minimum of five years.[134]

Informing Parents of their FERPA Rights: Educational agencies and institutions can be denied funds for failing to inform parents of their rights under FERPA.[135]

Enforcement: The Secretary of Education enforces FERPA. Funding only can be terminated, if there has been a failure to comply with FERPA's requirements and compliance cannot be obtained through voluntary means.[136]

Other Provisions: Other provisions of FERPA deal with disclosures of disciplinary proceedings, incidences of behaviors that pose a safety risk, information about registered sex offenders, and drug and alcohol violations.[137]

---

[131] 20 USC §1232g(b)(2)
[132] 20 USC §1232g(b)(3)
[133] 20 USC §1232g(b)(4)(A)
[134] 20 USC §1232g(b)(4)(B)
[135] 20 USC §1232g(e)
[136] 20 USC §1232g(f)
[137] 20 USC §1232g(b)(6)-(7), (h), (i)

Provisions Added by the USA Patriot Act: The USA Patriot Act,[138] enacted in response to the September 11, 2001 terrorist attacks, added a provision to FERPA permitting the U.S. Attorney General to apply with a court of competent jurisdiction for an ex parte order to require an educational institution to disclose education records where the request is made to investigate and prosecute domestic or international terrorism. Agencies that comply with such ex parte orders in good faith are not liable to any person for producing the requested records.[139]

Relevance for State Government:

FERPA's privacy requirements apply to educational agencies and institutions that receive funds under an applicable program of the Department of Education. Therefore, a state educational agency or institution that receives funds under an applicable program of the Department of Education is subject to FERPA's requirements.

Moreover, FERPA also applies specifically to state educational agencies or institutions regarding the right of a parent to inspect his or her child's education records. FERPA provides for the denial of applicable program funds for a state educational agency or institution that has a policy of denying or effectively prevents a parent from inspecting his or her child's education records maintained by that state agency or institution where the child attends or attended any school of the educational agency or institution that is subject to FERPA.

View the Text of FERPA at:
http://www4.law.cornell.edu/uscode/20/1232g.html

View the USA Patriot Act at:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

View a Red-Lined Version of FERPA by Piper, Marbury, Rudnick & Wolfe for the Center for Democracy and Technology at:
http://www.cdt.org/security/usapatriot/titlev.pdf

View the FERPA Regulations at:
http://www.ed.gov/offices/OM/fpco/ferpa/ferparegs.html

Related Links:

View the US Department of Education's FERPA Website at:
http://www.ed.gov/offices/OM/fpco/ferpa/index.html

---

[138] Public Law 107-56 §507, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf>.

[139] View a red-lined summary of FERPA as amended by the USA Patriot Act, Public Law 107-56 §507 at: <http://www.cdt.org/security/usapatriot/titlev.pdf>.

The Gramm-Leach-Bliley Act—Financial Services Modernization Act of 1999

In 1999, Congress enacted the Financial Services Modernization Act, also known as the "Gramm-Leach-Bliley Act" (hereinafter "the GLB Act"), as a means of removing the legal barriers that prevented mergers between banks, insurance companies, brokerage firms and other financial entities. The GLB Act has seven titles that mainly deal with modernizing the financial services industry.[140] Title V, Subchapter I of the GLB Act, 15 USC §§6801-6810,[141] provides additional protection to individuals' personal information that is collected, used and disclosed by banks and other entities in the financial services market. More specifically, Subchapter I places restrictions on the disclosure of individuals' nonpublic personal information. Additionally, Title V, Subchapter II of the GLB Act, 15 USC §§6821-6827,[142] assesses criminal penalties against those who fraudulently attempt to gain access to individuals' financial information. This summary provides an overview of the GLB Act's privacy provisions contained in Subchapters I and II of Title V.

Summary of the GLB Act's Disclosure of Nonpublic Personal Information Provisions:

Purpose: The GLB Act states that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[143]

Application: The GLB Act applies to "financial institutions,"[144] which are institutions that are "significantly engaged in financial activities."[145] Entities such as banks, savings and loans, credit unions, insurance companies, securities and commodities brokerage firms, mortgage brokers, check cashers, financial advisors, and credit counselors typically are considered to be "financial institutions."[146] It is important to note that governmental entities that provide financial products, such as mortgages or student loans, also may be covered by the GLB Act.[147]

Standards for Financial Institutions: To protect the privacy of nonpublic personal information held by financial institutions, the federal agencies that enforce the

---

[140] View a summary of the GLB Act's provisions at <http://www.senate.gov/~banking/conf/grmleach.htm>.
[141] View 15 USC §§6801-6810 at <http://www.ftc.gov/privacy/glbact/glbsub1.htm>.
[142] View 15 USC §§6821-6827 at <http://www.ftc.gov/privacy/glbact/glbsub2.htm>.
[143] 15 USC §6801(a)
[144] 15 USC §6809(3)(A)
[145] 16 CFR §313.3(k)(1), <http://www.ftc.gov/os/2000/05/65fr33645.pdf>.
[146] Federal Deposit Insurance Corporation (FDIC), "Privacy Choices: For Your Personal Financial Information," February 6, 2002, <http://www.fdic.gov/consumers/privacy/privacychoices/index.html>.
[147] Federal Trade Commission, Bureau of Consumer Protection, Division of Financial Practices, "The Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information," June 18, 2001, <http://www.ftc.gov/privacy/glbact/glboutline.pdf>.

GLB Act must establish standards for financial institutions within their jurisdiction to ensure that customer information is secure and confidential, to protect against threats to the security and integrity of customer information, and to protect against unauthorized access or use of such records that might result in substantial harm or inconvenience to the customer.[148] Agencies that must establish such standards include the Federal Trade Commission (FTC), the Federal Deposit Insurance Corporation (FDIC), the Securities and Exchange Commission (SEC), and even state insurance authorities.[149]

Nonpublic Personal Information: The purpose of the privacy provisions of the GLB Act are to protect nonpublic personal information. Nonpublic personal information is information which is personally identifying to the consumer and is obtained by a financial institution in one of the following ways: (1) from a consumer (2) from a transaction with the consumer or from a service performed for the consumer or (3) "otherwise obtained by the financial institution."[150] For practical purposes, nonpublic personal information may be most or all of the information that a financial institution has about a consumer. It even includes information obtained by financial institutions from other entities, such as credit bureaus.[151] Any lists, descriptions or groupings that financial institutions compile of consumers that are derived using nonpublic personal information are themselves considered nonpublic personal information.[152]

Notice Obligation of Financial Institutions to Consumers: Financial institutions generally cannot disclose directly or through an affiliate[153] nonpublic personal information to a nonaffiliated third party,[154] unless the financial institution provides a notice of its privacy policies (in accordance with §6803 of the GLB Act) and:

- Provides a clear and conspicuous written or electronic notice to the consumer that his or her nonpublic personal information might be disclosed to a nonaffiliated third party
- Gives the consumer an opportunity to "opt-out" or instruct the financial institution that his or her nonpublic personal information cannot be disclosed to a nonaffiliated third party, and
- Provides the consumer with a way to opt-out, if the consumer so chooses.[155]

Exceptions to the Opt-Out Requirements: Financial institutions can disclose consumers' nonpublic personal information without giving the consumer a right to refuse or opt-out of such disclosures in the following cases:

---

[148] 15 USC §6801(b)
[149] 15 USC §6805(a)
[150] 15 USC §6809(4)(A)
[151] Federal Trade Commission, Facts for Business, "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act," October 1, 2002, <http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm>.
[152] 15 USC §6809(4)(C)(i)
[153] An "affiliate" is "any company that controls, is controlled by, or is under common control with another company." See 15 USC §6809(6).
[154] A "nonaffiliated third party" is "any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution." See 15 USC §6809(5).
[155] 15 USC §6802(a)-(b)(1)

- Where the unaffiliated third party performs functions or services for the financial institution, including marketing the financial institution's products or services
- Where the unaffiliated third party and the financial institution have a joint marketing agreement.

In order to take advantage of the above-listed exceptions to the opt-out notice, financial institutions still must provide the consumer with notice of the disclosure and must enter into an agreement with the nonaffiliated third party to ensure that the confidentiality of the information is maintained.[156]

Exceptions to the Notice and Opt-Out Requirements: Under other GLB exceptions, financial institutions do not have to provide notice of their privacy policies, the fact of disclosure or information about a consumer's opt-out rights. These exceptions include the following:

- Where such disclosures are necessary to administer transactions requested or authorized by a consumer
- Where such disclosures are necessary to administer transactions in connection with servicing a consumer's account, servicing or processing a service or product requested or authorized by the consumer, or a securitization or secondary market sale
- Where the consumer grants his or her consent
- To protect the confidentiality or security of consumer records or to prevent fraud
- Disclosures to entities, such as law enforcement, the FTC, or state insurance authorities where such is permitted or required by law and is in accordance with the Right to Financial Privacy Act of 1978[157]
- Disclosures to a credit reporting agency or disclosures from a credit reporting agency under the Fair Credit Reporting Act
- To comply with federal, state or local legal requirements or investigations.[158]

Content of Privacy Notice: The privacy notice required under the GLB Act must contain the following elements of a financial institution's policies and practices:

- The disclosure of nonpublic personal information to affiliated and nonaffiliated third parties, including categories of disclosable information
- The disclosure of nonpublic personal information of former customers
- The protection of the nonpublic personal information of consumers
- The categories of persons to whom the information is or may be disclosed (note that this does not include disclosures made under the exceptions that allow disclosure without a privacy notice or notice of opt-out rights)
- The categories of nonpublic personal information that are collected by a financial institution

---

[156] 15 USC §6802(b)(2)
[157] The Right to Financial Privacy Act of 1978, 12 USC §3401 et seq., <http://caselaw.lp.findlaw.com/casecode/uscodes/12/chapters/35/toc.html>.
[158] 15 USC §6802(e)

- The protection of the confidentiality and security of nonpublic personal information
- Any disclosures required under the Fair Credit Reporting Act of communications among affiliates where the consumer has a right to opt-out.[159]

It is important to remember that, in situations where a financial institution would like to disclose a consumer's nonpublic personal information to a nonaffiliated third party, the financial institution also must provide notice of that fact along with notice of the consumer's right to opt-out of such disclosures and a means of opting-out if the consumer should so choose.[160]

Increase in Obligations in Cases of a Customer Relationship: A financial institution's notice obligation increases when dealing with a customer, as opposed to a consumer. For GLB Act purposes, a "consumer" is a person "who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes."[161] However, a "customer" is a person with whom a financial institution has a "continuing relationship" under which the financial institution provides one or more financial products or services for a customer's personal, family or household purpose.[162] Examples of *customer* relationships are where a customer has a credit or investment account with a financial institution or obtains a loan or purchases insurance products from a financial institution.[163] In contrast, instances where a *consumer* relationship exists are where a consumer obtains isolated financial transactions, such as ATM withdrawals or obtaining one-time personal or real property appraisal services.[164]

Where a customer relationship exists, a financial institution has the greater obligation of providing GLB Act disclosures at the time the customer relationship is established and annually thereafter for the duration of the customer relationship. Like the disclosures that must be made to a consumer where a financial institution would like to disclose the consumer's nonpublic personal information to a nonaffiliated third party, the disclosures to customers must be in a written or electronic form.[165]

Redisclosure Limitations: The general rule for the redisclosure of a customer or consumer's nonpublic personal information is that a nonaffiliated third party cannot directly or through an affiliate disclose such information to an entity that is unaffiliated with both the financial institution and the nonaffiliated third party to which the information initially was disclosed.[166]

However, exceptions to the general rule permit redisclosure to the affiliates of the financial institution and the nonaffiliated third party, which received the initial disclosure.

---

[159] 15 USC §6803. For more information on the Fair Credit Reporting Act disclosures, see 15 USC §1681a(d)(2)(A)(iii), <http://www.ftc.gov/os/statutes/fcrajan2002.pdf>.
[160] 16 CFR §313.6(a)
[161] 15 USC §6809(9)
[162] 16 CFR §313.3(h)(i)(1)
[163] 16 CFR §313.3(h)(i)(2)
[164] 16 CFR §313.3(h)(ii)
[165] 15 USC §6803(a)
[166] 15 USC §6802(c)

Other instances in which redisclosure is permitted depends upon how the nonaffiliated third party received the information in the first place from the financial institution:

- If the financial institution did not have to provide privacy and opt-out notices under a GLB Act exception when it initially disclosed the information, then the information can be redisclosed to carry out the exception in the ordinary course of business.
- If the financial institution provided the information outside of one of the GLB Act's exceptions (for example, where a consumer or customer failed to exercise his or her opt out rights), then the information can be redisclosed by the nonaffiliated third party to the extent that the financial institution can disclose it.[167]

Relation to State Laws: The GLB Act does not supercede, alter or affect state laws or regulations unless they are inconsistent. If a state law is inconsistent, then the state law only is superceded to the extent of its inconsistency with the GLB Act. States also can provide legal protections that are greater than those contained in the GLB Act as long as the FTC, after consultation with any other agencies with jurisdiction, determines that the state law or regulation is not inconsistent with the GLB Act.[168]

Enforcement: Depending upon the type of financial institution, the GLB Act prescribes which federal entity has enforcement jurisdiction. For example, the Office of the Comptroller of the Currency enforces the GLB Act for national banks. State insurance agencies also have enforcement jurisdiction against persons domiciled in their states who provide insurance. The FTC regulates the enforcement of the GLB Act against all other financial institutions that are not subject to another agency's enforcement jurisdiction.[169] It is important to note that the GLB Act provides that, where a state insurance regulator fails to adopt regulations to carry out the GLB Act, then the state will not be eligible to override the federal banking agency insurance customer protection regulations.[170]

Other Provisions of the GLB Act: Some other notable aspects of the GLB Act are:

- The GLB Act gives rulemaking authority to federal banking agencies, the FTC, the SEC, the Secretary of the Treasury, and the National Credit Union Administration, as necessary to carry out its provisions, and includes a requirement that these agencies coordinate their regulations to ensure consistency and comparability.[171]
- The rules promulgated under the GLB Act may provide for additional exceptions to the consumer notice and opt-out requirements as well as additional exceptions regarding the reuse of information and sharing of

[167] 16 CFR §313.11(a)-(b)
[168] 15 USC §6807
[169] 15 USC §6805(a)
[170] 15 USC §6805(c)
[171] 15 USC §6804(a)

account numbers, as long as such exceptions are consistent with the GLB Act's purposes.[172]

- The GLB Act does not in any way modify the Fair Credit Reporting Act.[173]
- The Secretary of the Treasury is required to conduct a study and report to Congress on information sharing practices among financial institutions and their affiliates by January 1, 2002, including recommendations for legal and administrative changes.[174]
- The GLB Act prohibits financial institutions from sharing consumer account numbers with nonaffiliated third parties for use in telemarketing, direct mail marketing or e-mail marketing. One notable exception is the disclosure of consumer account numbers to consumer reporting agencies.[175]

Summary of the GLB Act's Fraudulent Access to Financial Information Provisions:

Actions Criminalized by the GLB Act: The GLB Act criminalizes obtaining the customer information of a financial institution under false pretenses.[176] Specifically, the GLB Act makes it a crime to obtain the customer information of a financial institution or cause it to be disclosed in the ways listed below and also criminalizes any attempts to do so. Under the GLB Act, it is illegal to obtain customer information in any of the following ways:

- By making false, fictitious or fraudulent statements to a financial institution
- By making false, fictitious or fraudulent statements to a financial institution's customer, and
- By providing a financial institution with a document knowing that the document is forged, counterfeit, lost, stolen, fraudulently obtained or contains a fictitious, false or fraudulent statement or representation.[177]

The GLB Act also makes it a crime to request that another person obtain a customer's information from a financial institution, knowing that the person will obtain or make an attempt to obtain the information in the manner described above.[178]

The GLB Act specifies certain instances where conducting any of the above-described activities does not constitute a crime. Such instances include:

- Law enforcement agencies' obtaining of customer information from a financial institution in connection with performing their official duties
- A financial institution's obtaining of such information to test security procedures for maintaining the confidentiality of customer information, to investigate alleged employee misconduct or negligence or to recover customer

[172] 15 USC §6804(b)
[173] 15 USC §6806
[174] 15 USC §6808
[175] 15 USC §6802(d)
[176] Under this provision of the GLB Act, a "customer" is "a person…to whom the financial institution provides a product or service, including that of acting as a fiduciary." See 15 USC §6827(1). "Customer information of a financial institution" is "any information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer." See 15 USC §6827(2), <http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=15&sec=6827>.
[177] 15 USC §6821(a)
[178] 15 USC §6821(b)

information that was illegally obtained in violation of this Subchapter of the GLB Act

- An insurance institution's obtaining of such information for the investigation of insurance fraud where the investigation is legally authorized by the state
- A person's obtaining of a financial institution's customer information that is available as a public record filed pursuant to securities laws
- A state-licensed private investigator's obtaining of such information to the extent reasonably necessary to collect delinquent child support.[179]

Criminal Penalties: Knowing and intentional violations or attempted violations of this portion of the GLB Act can result in criminal fines under Title 18 of the United States Code as well as imprisonment for not more than 5 years.[180] The GLB Act raises the maximum criminal penalties in "aggravated cases" where a violation occurs while a person is violating another US law or where the GLB Act violation is part of a pattern of illegal activity that involves more than $100,000 within a one year period. In such cases, the criminal fine is doubled and the maximum incarceration period increases to not more than ten years.[181]

Administrative Enforcement: Generally, the FTC provides administrative enforcement of the GLB Act's criminal provisions regarding the obtaining of customer information under false pretenses. However, some federal agencies, such as the Office of the Comptroller of the Currency and the FDIC, are given enforcement responsibility over certain financial institutions within their jurisdiction.[182]

Relation to State Laws: This provision of Subchapter II is the same as the GLB Act's provision under Subchapter I. Hence, existing state laws are not affected as long as they are not inconsistent with the GLB Act. States also can provide greater legal protections as long as the FTC deems them not inconsistent with the GLB Act.[183]

Annual Reports to Congress: The FTC and Attorney General must submit an annual report to Congress on the number and disposition of enforcement actions taken under this provision of the GLB Act.[184]

---

[179] 15 USC §6821(c)-(g)
[180] 15 USC §6823(a). Title 18 of the United States Code specifies criminal fines. The amount of a criminal fine under Title 18 is dependent upon the classification of the offense. It appears that a fine for a GLB Act violation without aggravated circumstances would not be more than $250,000 for individuals. See 18 USC §3571(b)(3) and 18 USC §3559(4), <http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=3571> and <http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/ii/chapters/227/subchapters/a/sections/section_3559.html>.
[181] 15 USC §6823(b)
[182] 15 USC §6822
[183] 15 USC §6824
[184] 15 USC §6826(b)

Relevance to State Government:

Subchapter I of Title V of the GLB Act applies to "financial institutions." Where state governments are "significantly engaged" in financial activities, the GLB Act applies. An example of the financial activities of government entities that might fall under the GLB Act is where a government agency provides mortgages or student loans. As far as the enforcement of the GLB Act's nonpublic personal information disclosure restrictions, state insurance regulators may have jurisdiction over persons providing insurance in their state. Finally, the GLB Act's provisions in Subchapters I and II do not supercede consistent state laws. States have the option of providing greater privacy protections than the GLB Act provides as long as the FTC does not deem such state privacy protections as being inconsistent with the GLB Act.

View Title V, Subchapter I of the GLB Act (Disclosure of Nonpublic Personal Information) at: http://www.ftc.gov/privacy/glbact/glbsub1.htm

View Title V, Subchapter II of the GLB Act (Fraudulent Access to Financial Information) at: http://www.ftc.gov/privacy/glbact/glbsub2.htm

View the GLB Final Rule for Financial Privacy at:
http://www.ftc.gov/os/2000/05/65fr33645.pdf

View the GLB Final Rule for Safeguarding Information at:
http://www.ftc.gov/privacy/glbact/index.html

Related Links:

View the FTC Webpage on the GLB Act at:
http://www.ftc.gov/privacy/glbact/index.html

View the FTC Outline of the GLB Final Privacy Rule at:
http://www.ftc.gov/privacy/glbact/glboutline.pdf

View the FTC's "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act" at: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

View the FDIC's "Privacy Choices: For Your Personal Financial Information" at:
http://www.fdic.gov/consumers/privacy/privacychoices/index.html

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Summary:

In 1996, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to standardize the electronic exchange of health information and to improve the privacy and security of health information. HIPAA applies to health plans, health care clearinghouses, and health care providers who transmit health information electronically ("covered entities"). HIPAA authorizes the Secretary of Health and Human Services (HHS) to issue rules to accomplish the purpose of HIPAA.[185]

Overview of HIPAA and its Rules

The Secretary of Health and Human Services has promulgated the HIPAA rules on a phased-in basis. Many of the rules, such as the Transactions and Code Sets Rule, the Privacy Rule, and, most recently, the Security Rule, have been issued in their final form.[186] The compliance deadlines for these rules are:

- Transactions and Code Sets Rule: October 16, 2002 (for small health plans and covered entities that filed a compliance plan with HHS before October 16, 2002, the deadline is October 16, 2003)[187]
- Privacy Rule: April 14, 2003 (for small health plans, April 14, 2004)
- Security Rule: April 21, 2005 (for small health plans, April 21, 2006).[188]

Penalties of $100 per violation (up to a maximum of $25,000 per year for all violations of an identical requirement or prohibition) can be imposed for violation of the HIPAA rules. The knowing and wrongful disclosure of individually identifiable health information can result in a fine of up to $50,000 and a prison sentence of not more than one year. The maximum fine and prison term increases to a maximum fine of $100,000 and a prison sentence of not more than 5 years for violations committed under false pretenses. For violations committed with the intent to sell, transfer or use individually

---

[185] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, August 21, 1996, <http://hipaadvisory.com/regs/law/index.htm>.
[186] Status of HIPAA Regulations Compliance Calendar, hipaadvisory.com, March 2003, <http://hipaadvisory.com/regs/compliancecal.htm>.
[187] In December 2001, Congress enacted HR 3323, which extended the Transactions and Code Sets Rule compliance deadline by one year as long as a covered entity filed, by October 16, 2002, a compliance plan detailing, among other things: 1) an explanation of why the covered entity would not be in compliance by October 16, 2002, 2) a budget, schedule, work plan, and implementation strategy for compliance with the October 16, 2003 deadline, 3) any vendors or contractors that might be used in achieving compliance, and 4) a testing schedule to begin not later than April 16, 2003. View HR 3323 at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3323enr.txt.pdf>.
[188] Status of HIPAA Regulations Compliance Calendar, hipaadvisory.com, March 2003, <http://hipaadvisory.com/regs/compliancecal.htm>.

identifiable health information, the maximum penalty is a $250,000 fine and 10 years in prison.[189]

The HIPAA Privacy Rule

In accordance with HIPAA, Congress had the first opportunity to enact legislation governing privacy standards for individually identifiable health information. Since Congress did not enact these standards within 36 months after HIPAA's enactment, the Secretary of Health and Human Services was required to issue privacy standards.[190] In November 1999, HHS issued the Proposed Privacy Rule and, in December 2000, issued the Final Privacy Rule. However, in March 2002, HHS issued proposed modifications to the Privacy Rule "to ensure that [the Privacy Rule] protects privacy without interfering with access to care or quality of care." After a period for public comment, HHS issued the final modifications to the Privacy Rule in August 2002.[191] The following is a summary of the Final Privacy Rule's major provisions.[192]

Protected Health Information: The Privacy Rule covers medical records and other individually identifiable health information used or disclosed by an entity covered by HIPAA. The health information does not have to be in an electronic form, but can be in paper form or transmitted orally. However, the Privacy Rule excludes from the definition of protected health information educational records covered by the Family Educational Rights and Privacy Act. [193]

Hybrid Entities: For entities that provide some activities that are covered by HIPAA as well as some activities that are not covered by HIPAA, the Privacy Rule allows such entities to designate themselves as hybrid entities, which allows them more discretion in designating their healthcare components.[194]

Compliance Deadline: Covered entities, with the exception of small health plans, must be in compliance with the Privacy Rule by April 14, 2003 (those entities qualifying as "small health plans" must comply by April 14, 2004).[195]

Purpose of the Privacy Rule: Generally, the HIPAA Privacy Rule is intended to: 1) give patients greater control over their health information, 2) place limitations on the

---

[189] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, August 21, 1996.
[190] Ibid.
[191] HHS Fact Sheet: Protecting the Privacy of Patients' Health Information, US Department of Health and Human Services, August 21, 2002, <http://www.hhs.gov/news/press/2002pres/privacy.html>.
[192] The information for the summary of the Privacy Rule's major provisions can be found in the following two HHS Fact Sheets: "Protecting the Privacy of Patients' Health Information," August 21, 2002, <http://www.hhs.gov/news/press/2002pres/privacy.html> and "Modification to the Standards for Privacy of Individually Identifiable Health Information—Final Rule," August 9, 2002, <http://www.hhs.gov/news/press/2002pres/20020809.html>. Citations to the Final Privacy Rule are provided to indicate where more detailed information can be found, <http://www.os.dhhs.gov/ocr/combinedregtext.pdf>.
[193] 45 CFR §164.501. See also the Family Educational Rights and Privacy Act (FERPA), 20 USC §1232g , <http://www4.law.cornell.edu/uscode/20/1232g.html>.
[194] 45 CFR §164.504
[195] 45 CFR §164.534

use and release of medical records, 3) establish standards for safeguarding personal health information, and 4) provide for the disclosure of health information when a covered entity has a public responsibility to do so (such as under emergency circumstances).

Patient Consent for Use and Disclosure: Covered entities must provide patients with a written copy of their privacy practices as well as a notice of patient privacy rights.[196] Covered entity providers must make a good faith effort to obtain a patient's written acknowledgement of the privacy notice. As modified, the Privacy Rule makes patient consent optional for the disclosure and use of protected information for routine health purposes (treatment, payment, and health care operations). As originally drafted, the Privacy Rule required that patients consent to a healthcare provider's use and disclosure of protected health information prior to treatment.[197]

However, patient consent is required for the disclosure of HIPAA-protected information for non-routine disclosures, such as for marketing purposes. The rule's modifications streamlined the authorization requirements that formerly mandated that covered entities use different types of authorization forms. Covered entities now can use one authorization form. Patients must consent separately for each type of non-routine use or disclosure of their protected health information.[198]

Finally, the recent modifications to the Privacy Rule generally provide parents and legal guardians with access rights to their child's protected health information. However, the Privacy Rule modifications also clarified that state law or other applicable law governs where it specifically addresses disclosing the protected health information of a minor to his or her parent or guardian. Hence, where a state law prohibits or permits access by parents and/or guardians, then that state law governs as to parental or guardian access rights. In situations where the Privacy Rule does not grant access rights to a child's parent or guardian and no state law specifically provides for access by a parent or guardian, then covered entities have discretion to permit or deny access, as long as the decision is consistent with state or other applicable law.[199]

Limitations on Disclosure and Use of Protected Information: Generally, the Privacy Rule limits the amount of protected health information that can be used or disclosed to the minimum amount necessary to accomplish the purpose of the use or disclosure. However, exceptions to this provision of the Privacy Rule include where medical information is disclosed for treatment purposes (for example, where medical records are disclosed to a specialist or another physician for purposes of treating a patient). Also, where a patient authorizes the use or disclosure of protected information, then the covered entity does not have to comply with the minimum necessary requirement.[200]

To use or disclose protected patient information for marketing purposes, such as sending a patient marketing materials, a covered entity generally must obtain a patient's

[196] 45 CFR §164.520
[197] 45 CFR §164.506(b)(1)
[198] 45 CFR §164.508
[199] 45 CFR §164.502(g)
[200] 45 CFR §164.502(b)

written authorization.[201] Patient authorization also is needed where a covered entity sells patient lists or discloses protected information to a third party for the third party's marketing activities. However, doctors and other healthcare providers who communicate with patients during the course of treatment are not considered to be performing marketing activities.

Patient Access Rights: The HIPAA Privacy Rule generally gives patients the right to access their health information. For patients finding inaccuracies, the Privacy Rule provides that patients can request amendments to their health information.[202]

Privacy Safeguards on Personal Health Information: In order to ensure that personal health information is secure from improper disclosure and use, entities covered by HIPAA must adopt written privacy procedures establishing who can access personal health information, how a covered entity may use such information, and when disclosure of such information is permitted. Covered entities also must train their employees regarding their privacy procedures and must designate a privacy officer to ensure compliance with their privacy procedures.[203]

Business Associates: A covered entity can disclose protected health information to its business associates[204] and allow its business associates to create or receive such information as long as the covered entity documents, in a written agreement, its business associates' assurances to appropriately safeguard protected health information. The modification of the Privacy Rule provided covered entities with an additional year in which to alter their agreements with their business associates to comply with the Privacy Rule's requirements. [205]

Relation to State Law: The Privacy Rule provides that HIPAA preempts state laws that are contrary to HIPAA. However, exceptions apply in certain situations, such as where a state law is more stringent than HIPAA in protecting the privacy of individually identifiable health information or where a state law provides for the reporting of disease, injury, child abuse, birth or death. The Secretary of HHS has the authority to make exceptions to the general preemption rule where the Secretary determines that a state law is necessary:

- To prevent healthcare fraud and abuse
- To ensure the appropriate regulation by state authorities of insurance or health plans
- For healthcare reporting by the state on delivery or costs, or
- To serve a compelling public health, safety or welfare need.

The Privacy Rule provides a process for states to request an exception from the Secretary of HHS regarding the preemption of a state law. The Privacy Rule also provides

[201] 45 CFR §164.501 & §164.508(a)(3)
[202] 45 CFR §164.502(a)(1), (2)(i) and §164.524 & §164.526
[203] 45 CFR §164.530
[204] For a definition of what entities constitute a covered entity's "business associates," see 45 CFR §160.103.
[205] 45 CFR §160.103 and §164.502(e)

guidance as to when state laws are considered "contrary" to HIPAA or "more stringent" than HIPAA.[206]

The HIPAA Security Rule

General Purpose: In February 2003, HHS announced the finalization of the HIPAA Security Rule.[207] The deadline for compliance is April 21, 2005.[208] The final Security Rule standardizes the way covered entities protect the confidentiality, integrity, and availability of electronic protected health information. The Security Rule protects such information not only while held by a covered entity but also while it is in transit between covered entities and from covered entities to others.[209] Through this rule, HHS offered more of a model and general guidance for information security rather than provide detailed specifications. The rule emphasizes internal risk analysis and risk management.[210]

Overview of the Security Rule Requirements: The Security Rule requires that covered entities take the following measures:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information that covered entities create, receive, maintain or transmit
- Protect against any reasonably anticipated threats to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not otherwise permitted or required by the rule
- Ensure compliance by its workforce.[211]

Other provisions of the Security Rule provide for administrative safeguards, physical safeguards, technical safeguards, and business associate contracts.

The Transactions and Code Sets Rule

Background: The need for the Transactions and Code Sets Rule arose from the use of Electronic Data Exchange (EDI) by many in the healthcare industry to transfer electronically information in a standard format between trading partners. However, with an estimated 400 different formats in the U.S. for electronically processing health claims, HIPAA provides standardization for EDI by covered entities.[212]

---

[206] 45 CFR §160.202-§160.204
[207] 45 CFR Parts 160, 162 & 164, <http://www.hipaadvisory.com/regs/Regs_in_PDF/finalsecurity.pdf>.
[208] "HIPAA Fact Sheet on Security Standards Final Rule," HHS, February 24, 2003, <http://hipaadvisory.com/regs/finalsecurity/FinalSecurityFactSheet.doc>.
[209] "Security Standards: Background," Hipaadvisory.com, March 28, 2003, <http://hipaadvisory.com/regs/finalsecurity/background.htm>.
[210] "Summary Analysis: The Final HIPAA Security Rule," Tom Grove, Phoenix Health Systems, February 2003, <http://hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm>.
[211] 45 CFR §164.306, <http://www.hipaadvisory.com/regs/Regs_in_PDF/finalsecurity.pdf>.
[212] 45 CFR Parts 160 & 162 (Background), <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/finalrule/default.asp>.

General Purpose and Requirements: The Transactions and Code Sets Rule, in essence, "requires standardization of the data content by specifying uniform definitions of the data elements that will be exchanged in each type of electronic transaction and identification of the specific codes or values that are valid for each data element."[213] For covered entities that filed with HHS for a one-year extension, the compliance deadline is October 16, 2003. For those entities that did not file for an extension, the compliance deadline was October 16, 2002.

Application of the Rule: The Transactions and Code Sets Rule applies to health plans, health care clearinghouses, and health care providers who transmit electronically any health information in connection with a transaction covered by the rule.[214] Transactions coming within this rule would include health claims, health care payment, coordination of benefits, enrollment in a health plan, eligibility for a health plan, payment of health premiums, and referral certification and authorization.[215]

Recent Modifications: In February 2003, HHS issued modifications to the Transactions and Code Sets Rule, which broadly deal with the National Drug Code (repealing it for reporting drugs and biologics in non-retail transactions), retail pharmacy transactions, premium payments and coordination of benefits.[216]

Relevance of HIPAA for State Government:

HIPAA and its rules have important ramifications for state government because of the many state programs and agencies that might fall within the definition of a "covered entity." HIPAA affects the way in which covered entities exchange protected health information, ensure the privacy of protected health information, and secure that information. Overarching concerns for states regarding HIPAA include a lack of federal funding, a lack of federal guidance on the application and implementation of HIPAA, and the piecemeal promulgation of the HIPAA rules.

However, from a privacy perspective, the HIPAA Privacy Rule is important, because it sets a federal floor on the types of privacy safeguards that covered entities must have in place to protect health information. HIPAA specifically provides that the Privacy Rule only supercedes contrary state laws that are not as stringent as the Final Privacy Rule, meaning that more stringent state laws will remain valid and enforceable.

A recent NGA Issue Brief on HIPAA identifies concerns related to the Privacy Rule. Among them are concerns regarding what information is to be protected as health information, determining whether a state covered entity is complying with the restriction

---

[213] "Guide to Transactions and Code Sets Standards," Hipaadvisory.com, May 2000, <http://hipaadvisory.com/action/Compliance/Trans-CodeSetsGuide.htm>.
[214] 45 CFR §160.102
[215] "Guide to Transactions and Code Sets Standards," Hipaadvisory.com, May 2000.
[216] "Summary: Modifications to Standards for Electronic Transactions and Code Sets," Amanda Dorsey, Phoenix Health Systems, February 2003, <http://www.hipaadvisory.com/regs/finaltransmod/phssummary.htm>.

to limit disclosure to the minimum amount of information necessary, and determining what state laws are preempted by HIPAA.[217]

The recent finalization of the HIPAA Security Rule may enhance states' ability to formulate a more integrated approach to securing protected health information and protecting its privacy. The Security Rule, like the Privacy Rule, is important for states, because entities qualifying as HIPAA "covered entities" must meet the Security Rule's requirements by the April 21, 2005 deadline (April 21, 2006 for small health plans).

Finally, for those covered entities that are not small health plans or that did not file for an extension, the compliance deadline for the Transactions and Code Sets Rule expired in October 2002. In a 2002 Fact Sheet,[218] the National Governors Association identified several critical issues for states regarding the Transactions and Code Sets Rule. Among them were the following: (1) that states have the primary responsibility for determining which agencies qualify as "covered entities," and hence, must have to comply with the Transactions and Code Sets Rule (2) that states must identify in their business processes where HIPAA's standardized electronic transactions occur and whether to support implementation of HIPAA's standardized transactions by developing their own technology or using an information clearinghouse and (3) that states must abandon local billing codes that have been used to administer unique program features, such as benefit enhancements.

View the Text of the HIPAA Statute at: http://aspe.hhs.gov/admnsimp/pl104191.htm

Privacy Rule-Related Links:

View the HIPAA Final Privacy Rule (including the August 2002 Final Modifications) at:
http://www.os.dhhs.gov/ocr/combinedregtext.pdf

View the Final Modifications to the HIPAA Privacy Rule in the Federal Register at:
http://www.hhs.gov/ocr/hipaa/privrulepd.pdf

View a Fact Sheet of the HIPAA Final Modifications to the Privacy Rule at:
http://www.hhs.gov/news/press/2002pres/20020809.html

View Updated Frequently Asked Questions about the Privacy Rule at:
http://www.os.dhhs.gov/ocr/faqs1001.doc

View Searchable HIPAA Database of Frequently Asked Questions about the Privacy Rule at:

---

[217] Issue Brief, HIPAA & the States: Critical Issues and Compliance Strategies, NGA Center for Best Practices, May 28, 2002, <http://www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_4317,00.html>.

[218] "Fact Sheet: Standards for Electronic Transactions and Codes, Health Insurance Portability and Accountability Act of 1996 (HIPAA)," National Governors Association, Center for Best Practices, 2002, <http://www.nga.org/cda/files/HIPAA_TRANSACTIONS.pdf>.

http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php?p_sid=cQ3ub9Eg&p_lva=&p_li=&p_page=1&p_cat_lvl1=7&p_cat_lvl2=%7Eany%7E&p_search_text=&p_new_search=1

Security Rule-Related Link:

View the Final HIPAA Security Rule at:
http://www.hipaadvisory.com/regs/Regs_in_PDF/finalsecurity.pdf

Transactions and Code Sets Rule-Related Links:

View the Transactions and Code Sets Final Rule at:
http://www.hipaadvisory.com/regs/Regs_in_PDF/finaltrans.pdf

View the February 2003 Modifications of the Transactions and Code Sets Final Rule at:
http://www.hipaadvisory.com/regs/Regs_in_PDF/finaltransmod022003.pdf

Related Links:

NGA HIPAA Website:
http://www.nga.org/center/topics/1,1188,C_CENTER_ISSUE^D_4324,00.html

NGA Issue Brief "HIPAA & the States: Critical Issues and Compliance Strategies":
http://www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_4317,00.html

HHS Administrative Simplification Website:
http://aspe.os.dhhs.gov/admnsimp/

HHS's Office for Civil Rights Website:
http://www.hhs.gov/ocr/hipaa/

The Privacy Act of 1974

Summary:

The Privacy Act of 1974 is a broad statute that protects against unauthorized uses of records by federal agencies.[219] It regulates federal agencies' collection, maintenance, use and disclosure of personal information.[220] The Privacy Act was designed to address concerns over federal agencies' ability to investigate individuals, which was exposed during the Watergate scandal, and their increasing ability to store and retrieve personal information by using universal identifiers, such as Social Security Numbers (SSNs).[221] The Privacy Act, with the exception of a provision dealing with the disclosure of Social Security Numbers,[222] applies only to federal agencies. Neither the receipt of federal funds nor regulation by the federal government places a state or local agency within the Privacy Act's purview.[223]

General Disclosure Prohibitions and Exceptions: The Privacy Act prohibits the disclosure of federal agencies' records contained in a system of records that identify an individual and relate to such areas as education, financial transactions, medical history and criminal or employment history. However, an individual can consent in writing to disclosures.[224] The Privacy Act's prohibition on the disclosure of records has twelve enumerated exceptions that allow federal agencies to disclose an individual's personal information. Among the exceptions are disclosures:

- To employees of the agency maintaining the records who need the records to perform their duties
- Required by the federal Freedom of Information Act
- To specified federal agencies, including federal law enforcement agencies
- For routine uses that are compatible with the purpose of collecting the information.[225]

Protection of Information's Integrity and Accuracy: Other Privacy Act provisions seek to protect the integrity of personal information contained in federal agencies' databases, by requiring agencies to make detailed accountings of their disclosures under the Privacy Act's exceptions.[226] The Privacy Act also allows individuals to access records containing their own personal information and to amend the

---

[219] Privacilla.org, "The Privacy Act of 1974," August 28, 2000, <http://www.privacilla.org/government/privacyact.html>.
[220] US Department of Justice, "Overview of the Privacy Act of 1974: Introduction," May 2000, <http://www.usdoj.gov/04foia/04_7_1.html>.
[221] US Department of Justice, "Overview of the Privacy Act of 1974: Policy Objectives," May 2000.
[222] For more information on SSN disclosure prohibitions regarding state government, see the "Relevance for State Government" section of this summary.
[223] US Department of Justice, "Overview of the Privacy Act of 1974: Definitions—Agency," May 2000.
[224] 5 USC §552a(b), <http://www4.law.cornell.edu/uscode/5/552a.html>. Note that under, 5 USC §552a(a)(5) "a system of records" is "a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."
[225] 5 USC §552a(b). See also, US Department of Justice, "Overview of the Privacy Act of 1974: Conditions of Disclosure to Third Parties—Exceptions to the 'No Disclosure Without Consent' Rule," May 2000.
[226] 5 USC §552a(c)

information if it is inaccurate.[227] However, it permits the heads of federal agencies to promulgate rules that exempt the agencies from some of the Act's requirements.[228] The Privacy Act further provides that an individual's name and address may not be sold or rented by an agency, unless it is specifically authorized by law.[229] Agencies and individuals violating the Privacy Act may be subject to civil and criminal lawsuits.[230] Finally, the Privacy Act was amended in 1988 by the Computer Matching and Privacy Protection Act and again by additional amendments in 1990, which added provisions for agencies to follow in computer-matching activities.[231] Due to the detailed nature of the Computer Matching and Privacy Protection Act and related 1990 amendments, they are summarized separately in this Compendium.

Relevance for State Government:

Although the bulk of the Privacy Act applies only to federal agencies, §7 of the Privacy Act applies to federal, state and local agencies. It prohibits agencies from denying an individual any right, benefit or privilege because of his or her refusal to disclose a Social Security Number (SSN). However, this broad prohibition does have several exceptions. The prohibition does not apply to any disclosure mandated by a federal statute. Moreover, federal, state and local agencies maintaining a system of records that was in existence and operating before January 1, 1975, do not have to comply with this prohibition, as long as the SSN disclosures were required under a statute or regulation adopted prior to that date and used in order to verify the identity of an individual. Note that the Tax Reform Act of 1976 expressly exempts state agencies from the prohibition to the extent that they use SSNs in administering taxes, public assistance, driver's licenses and motor vehicle registration laws. However, federal, state and local agencies that request that an individual disclose his or her SSN are required to inform that individual of the following:

- Whether the SSN disclosure is mandatory or voluntary
- The statutory authority under which the agency is requesting the SSN
- What uses will be made of the SSN.[232]

Finally, two Privacy Act exceptions may be of state interest. State and local government agencies may be able to obtain federal records under the Privacy Act's exceptions for law enforcement activities upon the request for such records by the agency's head. Moreover, any court of "competent jurisdiction" can order that federal agencies' records be disclosed.[233]

---

[227] 5 USC §552a(d)
[228] 5 USC §552a(j)-(k)
[229] 5 USC §552a(n)
[230] 5 USC §552a(g)-(i)
[231] 5 USC §552a(o). See also US Department of Justice, "Overview of the Privacy Act of 1974: Computer Matching," May 2000.
[232] 5 USC §552a notes "Disclosure of Social Security Number," <http://www4.law.cornell.edu/uscode/5/552a.notes.html> & US Department of Justice, "Overview of the Privacy Act of 1974: Social Security Number Usage," May 2000. Note that this provision was never codified in the United States Code.
[233] 5 USC §552a(b). See also, US Department of Justice, "Overview of the Privacy Act of 1974: Conditions of Disclosure to Third Parties—Exceptions to the 'No Disclosure Without Consent' Rule," May 2000.

View the Privacy Act of 1974 at: http://www4.law.cornell.edu/uscode/5/552a.html.

View the Privacy Act's Note on the Disclosure of Social Security Numbers at:
http://www4.law.cornell.edu/uscode/5/552a.notes.html

View Summaries of the Privacy Act of 1974 at:

U.S. Department of Justice: http://www.usdoj.gov/04foia/04_7_1.html.

Privacilla.org: http://www.privacilla.org/government/privacyact.html.

Disclaimer

NASCIO makes no endorsement, express or implied, of any links to websites contained herein, nor is NASCIO responsible for the content or the activities of any linked sites. Any questions should be directed to the administrators of the specific sites to which this publication provides links.

While NASCIO has made all reasonable attempts to ensure that the information contained in this publication and links to other information are correct, NASCIO does not represent or guarantee the correctness of the information contained herein or any linked information presented, referenced or implied. All critical information should be independently verified.

This publication is not intended to provide legal advice. Please consult your general counsel for the application of the laws summarized herein to your individual situation.