Federal Privacy Laws and Regulations

Summary of the six key Federal privacy laws and regulations for VA:

Freedom of Information – FOIA (5 U.S.C. 552)	• Requires all agencies of the executive branch to disclose Federal agency records or information upon receiving a written request for them from any individual except for those records or portions of them that are protected from disclosure by certain exemptions and exclusions. • Any record may be obtained through the FOIA, provided that the record is not exempt from release by one of the nine FOIA exemptions. In the case of Privacy Act records, if you are not the subject of the record, you must provide the written permission of the individual whose records you seek. (Medical and beneficiary records are Privacy Act records and some of the information is exempt from release under some of the exemptions.) If the individual is deceased, you must provide a copy of the death certificate. In no case will the names and/or addresses of beneficiaries (including deceased beneficiaries) be released (per the VA Claims Confidentiality Statute, 38 U.S. C. 5701). • Types of records include medical, benefit, personnel, burial, financial, audits, administrative investigations, legal opinions, and contracts. http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm
Privacy Act of 1974 (5 U.S.C. 552a)	• Balances the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them. It covers information that can be retrieved by an individual's name or other identifier from systems of records (*i.e.,* social security number; date of birth, etc.). • Defines the following: o ***Record*** – "any item, collection, or grouping of information about an individual that is maintained by an agency, including but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." o ***System of Records*** – "a group of any records under the control of any 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." • In general, applies only to Federal agencies. • Provides an individual the following rights: o To access, review, and obtain copies the Federal government maintains on him or her o To request an amendment to records that are incorrect o To obtain an accounting or list of disclosures of information maintained on him or her • Restricts disclosures of personally identifiable information maintained by the Federal government (there are 12 exceptions). • Creates the basis for a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records. • Applies to systems that contain the records of ten or more individuals. http://vaww.vhaco.va.gov/privacy/Documents/5USC552a.htm

Health Insurance Portability and Accountability Act – HIPAA Privacy Rule (45 CFR Parts 160 and 164)	• Applies to VHA and VHA systems only • Provides confidentiality for VHA patients' protected health information (PHI). • Allows VHA to use or disclose information without a patient's prior written authorization for VHA treatment, payment, or health care operations. • Prohibits other uses and disclosures of PHI except as authorized by the regulation or with a prior written authorization. • Provides additional rights to the individual to whom the PHI pertains: o Request to restrict how PHI is used o Review and receive a copy of health information o Request an amendment to health information o Request health information be communicated in a confidential manner o Ability to file a complaint if privacy rights were violated http://www.hhs.gov/ocr/hipaa/privrulepd.pdf (Text of Privacy Rule) http://www.hhs.gov/ocr/privacysummary.pdf (Summary of Privacy Rule) http://www.hhs.gov/ocr/hipaa/ (HHS, Office of Civil Rights HIPAA web page)
The VA Claims Confidentiality Statute (38 U.S.C. 5701)	• Provides for the confidentiality of all VHA patient claimant information, with special protection for their names and home addresses. • Provides for the same for information about their dependents. Prohibits disclosure of these names and addresses except as authorized by the statute. • Does not apply to employee information. http://vaww.vhaco.va.gov/privacy/Documents/38USC5701.htm
Confidentiality of Healthcare Quality Assurance Review Records (38 U.S.C. 5705)	• Provides for the confidentiality of Healthcare Quality Assurance (QA) Review Records. • Records created by VHA as part of a designated medical quality-assurance program are confidential and privileged. • VHA may disclose this data in only a few, limited situations. http://vaww.vhaco.va.gov/privacy/Documents/38USC5705.htm
Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection With the Human Immunodeficiency Virus (HIV), and Sickle Cell Anemia Medical Records (38 U.S.C. 7332)	• The most restrictive of the privacy laws and applies only to VA. • Provides for the confidentiality of VHA-created, individually-identifiable Drug Abuse, Alcoholism and Alcohol Abuse, Infection with the Human Immunodeficiency Virus, and Sickle Cell Anemia Medical Records and Health Information. • Prohibits use or disclosure with a few exceptions. VHA may use the information to treat the VHA patient who is the record subject. • Must have specific written authorization in order to disclose in most cases, including for treatment by non-VA provider. • http://vaww.vhaco.va.gov/privacy/Documents/38USC7332.htm

Other major privacy laws and regulations:

Children's On-line Privacy Protection Act – COPPA	Applies to the online collection of personal information from children under 13. It spells out what the web site operator must do: • **Post a privacy policy** on the homepage of the website and link to the privacy policy everywhere personal information is collected. • **Provide notice to parents** about the site's information collection practices and, with some exceptions, get verifiable parental consent ***before*** collecting personal information from children. • **Give parents the choice to consent** to the collection and use of a child's personal information for internal use by the website, and give them the chance to choose not to have that personal information disclosed to third parties. • **Provide parents with access** to their child's information, and the opportunity to delete the information and opt out of the future collection or use of the information. • **Not condition a child's participation** in an activity on the disclosure of more personal information than is reasonably necessary for the activity. • **Maintain the confidentiality, security and integrity** of the personal information collected from children. http://www.ftc.gov/ogc/coppa1.htm
Clinger-Cohen Act	This act includes the Information Technology Management Reform Act and the Federal Acquisition Reform Act of 1996, which were included in the National Defense Authorization Act for Fiscal Year 1996 (see pages 458 and 495 in the link below). • Requires major Federal agencies to establish the position of Chief Information Officer (CIO) with clear authority, responsibility, and accountability for the agency's information resources management. • Requires National Institute of Standards and Technology (NIST) to promulgate standards and guidelines for Federal computer systems, which include the security and privacy of Federal computer systems. • Information technology investments should: o Support the agency's core mission o Be consistent with the agency's architecture o Reflect a portfolio management approach o Reduce risks and enhance manageability http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104.pdf
Computer Matching and Privacy Protection Act	• Computer matching is the computerized comparison of information about individuals for the purpose of determining eligibility for Federal benefit programs. o **Matching program** – is the computerized comparison of: (1) two or more automated systems of records with a set of non-Federal records; or (2) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with a set of non-Federal records. It excludes certain tax refund offset programs from such definition. • Requires Federal agencies to enter into written agreements with other agencies or non-Federal entities before disclosing records for use in computer matching programs. These agreements are available to the public upon request. • Specifies areas to be addressed in such agreements, including justification for matching, notifying individuals whose records are to be matched, procedures for retention and destruction of data after matching, and prohibitions on disclosure of records and the compilation of data.

	• Prohibits an agency from taking adverse action against someone as a result of information produced by the programs until the agency has verified such information and provided the person due process (these sections only were amended slightly in 1990). http://ows.doleta.gov/dmstree/uipl/uipl90/uipl_0490.htm#up0490a
The E-Government Act of 2002	The privacy provisions were included in Title II, Section 208 (pages 23-25 in the link below). • **Privacy Impact Assessments** – A PIA is an analysis that seeks to identify and mitigate the privacy risks associated with the use of personal information by a project or system. o Federal agencies are required to conduct privacy impact assessments (PIAs) prior to developing or procuring information technology systems that collect, maintain, or disseminate information about the public. o Once completed, the Chief Information Officer, or an equivalent officer, must review them and make them publicly available. o VA's PIAs can be found at http://www.va.gov/oit/egov/privacy/pia.asp. • **Web-page privacy policy** – Federal agencies must include a machine-readable privacy policy on agency websites the public uses. VA's web page privacy policy can be found at http://www.va.gov/privacy/. Also, Federal agencies' privacy policy notices must be consistent with the privacy policy requirements of the Privacy Act. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf
Federal Information Security Management Act – FISMA	FISMA was included as Title III of the E-Government Act of 2002 (pages 48-63 in the link below). • The goals of FISMA include the development of a comprehensive framework to protect the government's information, operations, and assets. • FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) in order to strengthen information technology system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level. • To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with FISMA. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf (see pages 48-63)
Government Paperwork Elimination Act	This was included as Title XVII of the Omnibus Appropriations Act for Fiscal Year 1999, Public Law 105-277. • Requires Federal agencies to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. • Specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives. • Requires OMB, with NIST, to conduct on-going study of use of electronic signatures on individual privacy. • http://www.cio.gov/Documents/paperwork_elimination_act.html

Gramm-Leach-Bliley Act	Officially called the Financial Modernization Act of 1999, this includes provisions to protect consumers' personal financial information held by financial institutions. (For VA – in general, applies to VBA loan programs only.) • Requires clear disclosure of privacy policies by all financial institutions regarding the sharing of non-public personal information with both affiliates and third parties. • Disclosure is required to take place at the time of establishing a customer relationship; not less than annually, thereafter. • Establishes consumer opt-out rights. • Requires administrative, technical and physical safeguards to maintain the security, confidentiality, and integrity of the information. • Requirements apply to non-affiliated third parties who maintain financial information. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf
OMB Circular A-130 – Management of Federal Information Resources	Office of Management and Budget guidance: • Establishes policy for the management of Federal information resources. • Includes detailed appendices on the following: o Federal agency responsibilities for maintaining records about individuals o Security of Federal automated information systems http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
OMB Memorandum M-03-22	Office of Management and Budget guidance on how to implement the privacy provisions of the E-Government Act. http://www.whitehouse.gov/omb/memoranda/m03-22.html
OMB Memorandum M-99-18	OMB guidance on posting clear privacy policies on web pages (implementation of the web page policies of the E-Government Act). http://www.whitehouse.gov/omb/memoranda/m99-18.html
OMB Memorandum M-00-13	OMB guidance on when agencies can use persistent "cookies" on Federal websites (Implementation of web page policies of the E-Government Act). http://www.whitehouse.gov/omb/memoranda/m00-13.html
OMB Memorandum M-01-05	Guidance on computer-matching and computer matching activities http://www.whitehouse.gov/omb/memoranda/m01-05.html
Paperwork Reduction Act	• Establishes a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner • Requires each Federal data collection form to explain why the information is being collected, how it is to be used, and whether the individual's response is mandatory (required by law), required to obtain a benefit, or voluntary. • Agencies must ensure disclosure policies will honor any claims of confidentiality on forms http://www.cio.noaa.gov/itmanagement/pralaw.pdf