Privacy

Laws

and

References

NIH Privacy Laws and References (May 2012)
# Table of Contents

Legislative Drivers (Public Laws): .................................................................................................................................................. 1  
Presidential Directives: ........................................................................................................................................................................ 3  
Federal Regulations: ............................................................................................................................................................................. 4  
  - Code of Federal Regulations (CFR): .................................................................................................................................................. 4  
  - Federal Acquisition Regulations (FAR): ......................................................................................................................................... 4  
  - Health and Human Services Acquisition Regulations (HHSAR): ................................................................................................. 4  
Federal Publications: .................................................................................................................................................................................. 6  
  - Federal Information Processing Standards (FIPS): ............................................................................................................................... 6  
  - National Institute of Standards and Technology (NIST): .................................................................................................................. 6  
Office of Management and Budget Guidance (OMB): ............................................................................................................................ 8  
  - OMB Circulars: .................................................................................................................................................................................... 8  
  - OMB Memoranda: ............................................................................................................................................................................... 8  
    - Calendar Year 2011: ........................................................................................................................................................................... 8  
    - Calendar Year 2010: ........................................................................................................................................................................... 8  
    - Calendar Year 2009: .......................................................................................................................................................................... 9  
    - Calendar Year 2008: .......................................................................................................................................................................... 9  
    - Calendar Year 2007: .......................................................................................................................................................................... 9  
    - Calendar Year 2006: .......................................................................................................................................................................... 10  
    - Calendar Year 2005: .......................................................................................................................................................................... 10  
    - Calendar Year 2004: .......................................................................................................................................................................... 11  
    - Calendar Year 2003: .......................................................................................................................................................................... 11  
    - Calendar Year 2002: .......................................................................................................................................................................... 12  
    - Calendar Year 2001: .......................................................................................................................................................................... 12  
    - Calendar Year 2000: .......................................................................................................................................................................... 12  
    - Calendar Year 1999: .......................................................................................................................................................................... 13  
    - Calendar Year 1998: .......................................................................................................................................................................... 13  
HHS Privacy Policy: .................................................................................................................................................................................. 14  
HHS Cybersecurity Program Privacy Documents: ................................................................................................................................. 15  
NIH Policy, Provisions & Guidelines: ..................................................................................................................................................... 17  
National Archives and Records Administration (NARA): ............................................................................................................................. 19  
Training: ................................................................................................................................................................................................. 20  
Websites: ................................................................................................................................................................................................. 21  
  - Health and Human Services (HHS): ................................................................................................................................................... 21  
  - National Institutes of Health (NIH): ............................................................................................................................................... 21  
Other Useful Websites: ............................................................................................................................................................................ 23
Legislative Drivers (Public Laws):

  http://www.coppa.org/coppa.htm
  http://www.coppa.org/comply.htm


  http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+18USC1030

  http://www.whitehouse.gov/omb/inforeg/final_guidance_pl100-503.pdf


  http://www2.ed.gov/policy/gen/reg/ferpa/index.html and
  http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+20USC1232g


  http://uscode.house.gov/download/pls/44C33.txt
  http://www.nih.gov/icd/od/foia/efoia.htm


  http://www.ftc.gov/privacy/glbact/glbsub1.htm


  http://ocio.nih.gov/itmra/itmra96.html


  http://www.justice.gov/opcl/privstat.htm

  http://www.access-board.gov/sec508/guide/act.htm
Presidential Directives:

Federal Regulations:

**Code of Federal Regulations (CFR):**

- 45 CFR, Part 5b, HHS Privacy Act Regulations:  
  [http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=d8c05a9cf0b3dd219f61ecf068cb7260&rgn=div5&view=text&node=45:1.0.1.1.7&idno=45](http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=d8c05a9cf0b3dd219f61ecf068cb7260&rgn=div5&view=text&node=45:1.0.1.1.7&idno=45)

**Federal Acquisition Regulations (FAR):**

- FAR Part 1.602-1(b), Career Development, Contracting Authority, and Responsibilities:  

- FAR Part 24, Protection of Privacy and Freedom of Information:  
  [http://www.acquisition.gov/far/current/html/Subpart%2024_1.html#wp1074189](http://www.acquisition.gov/far/current/html/Subpart%2024_1.html#wp1074189)

- FAR Part 39.105, Privacy:  
  [http://www.acquisition.gov/far/current/html/Subpart%2039_1.html#wp1096819](http://www.acquisition.gov/far/current/html/Subpart%2039_1.html#wp1096819)

- FAR Part 39.107, Contract Clause:  
  [http://www.acquisition.gov/far/current/html/Subpart%2039_1.html#wp1096819](http://www.acquisition.gov/far/current/html/Subpart%2039_1.html#wp1096819)

- FAR Part 52.224-1, Privacy Act Notification:  

- FAR Part 52.224-2, Privacy Act:  

- FAR Part 52.239-1, Privacy or Security Safeguards:  

**Health and Human Services Acquisition Regulations (HHSAR):**

- HHSAR Part 324, Protection of Privacy and Freedom of Information:  
  [http://www.access.gpo.gov/nara/cfr/waisidx_02/48cfr324_02.html](http://www.access.gpo.gov/nara/cfr/waisidx_02/48cfr324_02.html)

- HHSAR Part 352.224-70, Confidentiality of Information:  
Office of the Senior Official for Privacy

- HHSAR Part 352.270-12, Privacy Act:
Federal Publications:

**Federal Information Processing Standards (FIPS):**


**National Institute of Standards and Technology (NIST):**


- NIST Special Publications (SP), Complete list of NIST Publications: [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)


Office of Management and Budget Guidance (OMB):

**OMB Circulars:**

- Office of Management and Budget Circular A-11, Section 53, Information Technology and E-Government:  

- OMB Circular A-130, Management of Federal Information Resources (November 28, 2000):  
  [http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html](http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

**OMB Memoranda:**

**Calendar Year 2011:**

- M-11-02, Sharing Data While Protecting Privacy (November 3, 2010):  

**Calendar Year 2010:**


- M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010):  


  [http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf)
Calendar Year 2009:


Calendar Year 2008:


Calendar Year 2007:


Calendar Year 2006:

- M-06-26, Suspension and Debarment, Administrative Agreements, and Compelling Reason Determination (August 31, 2006):


- M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006):

- M-06-16, Protection of Sensitive Agency Information (June 23, 2006):

- M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006):

  [http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-06.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-06.pdf)

Calendar Year 2005:

http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-17.pdf

http://www.whitehouse.gov/omb/memoranda_fy2005_m05-15/

M-05-08, Designation of Senior Agency Officials for Privacy (February 11, 2005):
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf

M-05-05, Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services (December 20, 2004):
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-05.pdf


Calendar Year 2004:

http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-25.pdf

http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-25_template.xls

http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf

Calendar Year 2003:

http://www.whitehouse.gov/omb/memoranda_m03-22/


Calendar Year 2002:


• M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones (October 17, 2001): http://www.whitehouse.gov/omb/memoranda_m02-01/

Calendar Year 2001:


• M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (December 20, 2000): http://www.whitehouse.gov/omb/memoranda_m01-05/

Calendar Year 2000:

• M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000): http://www.whitehouse.gov/omb/memoranda_m00-13/

• M-00-07, Incorporating and Funding Security in Information Systems Investments (February 28, 2000): http://www.whitehouse.gov/omb/memoranda_m00-07/
Calendar Year 1999:


Calendar Year 1998:

HHS Privacy Policy:

- HHS Policy for Internet Domain Names: http://www.hhs.gov/policies/webpolicies/200501.html
- HHS Policy for Section 508 Compliance: http://www.hhs.gov/web/508/
HHS Cybersecurity Program Privacy Documents:

- HHS-OCIO Policy for Information Systems Security and Privacy (IS2P):

- HHS-OCIO Policy for Social Media Technologies:
  http://www.hhs.gov/ocio/policy/policy_2010-0003-_ocio.html

- HHS-OCIO Memo for the Implementation of OMB M-10-22 and 23:
  http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/PC/memo_implementation_of_omb_m_10_22_and_m_10_23_pdf.pdf

- HHS-OCIO Guide for Using Web Measurement and Customization Technologies:

- HHS-OCIO Policy for Information Systems Security and Privacy (IS2P) Handbook:
  http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/PISSP/policy_for_info_sys_sec_and_priv_hndbk_20110707.pdf

- HHS-OCIO Policy for Privacy Impact Assessment (PIA):
  http://www.hhs.gov/ocio/policy/20090002.001.html

- HHS Policy for Responding to Breaches of Personally Identifiable Information (PII):

- HHS-OCIO Policy for IT Security and Privacy Incident Reporting and Response:
  http://www.hhs.gov/ocio/policy/hhs_ocio_policy_2010_0004.html

- HHS-OCIO-Policy for Machine-Readable Privacy Policies:
  http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/MRPPG/mrpp_guide.pdf

- HHS-OCIO Incident Management and Response Website:
  http://www.hhs.gov/ocio/securityprivacy/incidentmanagement/incidentresp.html

- HHS Updated Departmental Standard for the Definition of Sensitive Information

- Machine-Readable Privacy Policy FAQs:
  http://intranet.hhs.gov/it/cybersecurity/docs/privacy/MRFAQ/mrpp_faq.pdf

- Privacy in the System Development Lifecycle (SDLC):
  http://intranet.hhs.gov/it/docs/privacy/PSDLC/Privacy_in_SDLC.html
• Privacy Tri-Fold Brochure:
  http://intranet.hhs.gov/infosec/docs/privacy/Trifold/Privacy_Tri-fold.pdf
NIH Policy, Provisions & Guidelines:

- NIH Manual Chapter 1130, Delegations of Authority: Program, General 4B, Privacy Act Appeals:  

- NIH Manual Chapter 1183, NIH Publications and Audiovisuals: Preparation, Review, Approval, and Distribution:  

- NIH Manual Chapter 1184, Scientific, Technical, and Other Professional Information Presented by NIH Employees: Review, Approval, and Distribution:  

- NIH Manual Chapter 1186, Use of NIH Names and Logos:  

- NIH Manual Chapter 1743, NIH Records Control Schedule “Keeping and Destroying Records”:  

- NIH Manual Chapter 1744, NIH Vital Records Program:  

- NIH Manual Chapter 1745, NIH Information Technology (IT) Privacy Program:  

- NIH Manual Chapter 1745-1, NIH Privacy Impact Assessments:  

- NIH Manual Chapter 1754, Reporting Allegations of Criminal Offenses, Misuse of NIH Grant and Contract Funds, or Improper Conduct by an NIH Employee:  

- NIH Manual Chapter 1825, Information Collection from the Public:  

- NIH Manual Chapter 2400-01, Introduction to Government Ethics at the NIH:  
  http://www1.od.nih.gov/oma/manualchapters/ethics/2400-01/

- NIH Manual Chapter 2400-04, Managing Conflicts of Interests and the Introduction of Bias:  
  http://www1.od.nih.gov/oma/manualchapters/ethics/2400-04/


National Archives and Records Administration (NARA):


Training:

- HHS Privacy Awareness Training: http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/awarenesstraining.html
- HHS Security Education and Awareness Website: http://intranet.hhs.gov/it/cybersecurity/training/index.html
- NIH Privacy Awareness Training:
- NIH Information Security Awareness Training: http://irtsectraining.nih.gov/
Websites:

**Health and Human Services (HHS):**

- HHS Cybersecurity Program Online Web Page:  
  [http://intranet.hhs.gov/infosec](http://intranet.hhs.gov/infosec)

- HHS ProSight-FISMA Database:  
  [https://sport.hhs.gov/prosight/](https://sport.hhs.gov/prosight/)

- HHS ProSight Form:  

- HHS Office of Civil Rights Web Page:  

- HHS Residual Standards of Conduct:  
  [http://ethics.od.nih.gov/LawReg/HHS-Resid-Std.HTM](http://ethics.od.nih.gov/LawReg/HHS-Resid-Std.HTM)

- HHS Supplemental Standards of Ethical Conduct for Employees of DHHS:  
  [http://ethics.od.nih.gov/LawReg/5cfr5501.pdf](http://ethics.od.nih.gov/LawReg/5cfr5501.pdf)

**National Institutes of Health (NIH):**

- NIH Information Technology General Rules of Behavior:  

- NIH Privacy Web Page:  

- NIH Privacy SharePoint Website (NIH Employees Only):  

- NIH Office of the CIO website:  

- NIH Encryption Web Page:  

- NIH ISSO Corner:  
• NIH IT Incident Response and Prevention:  

• NIH Records Management Web Page:  
  http://oma.od.nih.gov/ms/records/

• NIH FOIA Web Page:  
  http://www.nih.gov/icd/od/foia/

• NIH HIPAA Web Page:  
  http://privacyruleandresearch.nih.gov/

• NIH OMB Project Clearance Web Page:  
  http://odoerdb2.od.nih.gov/oer/policies/project_clearance/pcb.htm

• NIH Personally Identifiable Information (PII) Protection Web Page:  
  http://ocio NIH.gov/security/PIIProtection.html

• NIH Privacy Act Systems of Records (SOR) Notices:  
  http://oma.od.nih.gov/ms/privacy/pa-files/read02systems.htm

• NIH ProSight-FISMA Web Page:  
  https://ocio.nih.gov/nihsecurity/ProSight-FISMA-info.htm

• NIH Website Privacy Policy Statement:  
  http://www.nih.gov/about/privacy.htm

• NIH Ethics Program:  
  http://ethics.od.nih.gov/

• NIH Encryption Web Page:  
Other Useful Websites: