Privacy

Laws

and

References
# Table of Contents

Legislative Drivers (Public Laws): ................................................................. 1  
Presidential Directives & Executive Orders: ............................................... 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: .................................................................................. 5  
  - Federal Information Processing Standards (FIPS): ............................ 5  
  - National Institute of Standards and Technology (NIST): .................... 5  
Office of Management and Budget Guidance (OMB): .............................. 7  
  - OMB Circulars: .................................................................................. 7  
  - OMB Memoranda: ............................................................................. 7  
    - Fiscal Year 2017: ............................................................................ 7  
    - Fiscal Year 2016: ............................................................................ 8  
    - Fiscal Year 2015: ............................................................................ 8  
    - Fiscal Year 2014: ............................................................................ 9  
    - Fiscal Year 2013: ............................................................................ 9  
    - Fiscal Year 2012: ............................................................................ 9  
    - Fiscal Year 2011: ............................................................................ 9  
    - Fiscal Year 2010: ............................................................................ 9  
    - Fiscal Year 2008: ........................................................................... 10  
    - Fiscal Year 2006: ........................................................................... 10  
    - Fiscal Year 2005: ........................................................................... 10  
    - Fiscal Year 2004: ........................................................................... 11  
    - Fiscal Year 2003: ........................................................................... 11  
    - Fiscal Year 2002: ........................................................................... 11  
    - Fiscal Year 2001: ........................................................................... 12  
    - Fiscal Year 2000: ........................................................................... 12  
    - Fiscal Year 1999: ........................................................................... 12  
    - Fiscal Year 1998: ........................................................................... 12  
  - HHS Privacy Policy: ............................................................................ 13  
  - HHS Cybersecurity Program Privacy Documents: .............................. 14  
  - NIH Policy, Provisions & Guidelines: ................................................. 16  
  - National Archives and Records Administration (NARA): .................... 18  
  - Training: .......................................................................................... 19  
  - Websites: .......................................................................................... 20  

NIH Privacy Laws and References (July 2017)
National Institutes of Health

Office of the Senior Official for Privacy

Health and Human Services (HHS): ................................................................. 20
National Institutes of Health (NIH): ............................................................ 20
Other Useful Websites: ............................................................................. 22
Legislative Drivers (Public Laws):

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


- Federal Information Technology Acquisition Reform Act (FITARA) of 2014, (10 U.S.C 11319) (February 25, 2014): https://olao.od.nih.gov/content/about-fitara

http://www.nih.gov/icd/od/foia/efoia.htm


https://www.dol.gov/ocfo/media/regs/ITMRA.pdf


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


https://www.congress.gov/114/bills/hr6/BILLS-114hr6rfs.pdf
Presidential Directives & Executive Orders:


Federal Regulations:

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


**Federal Acquisition Regulations (FAR):**

- FAR Part 52.239-1, Privacy or Security Safeguards: [https://www.acquisition.gov/far/html/52_233_240.html](https://www.acquisition.gov/far/html/52_233_240.html)

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

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

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (April 2013): [http://dx.doi.org/10.6028/NIST.SP.800-53r4](http://dx.doi.org/10.6028/NIST.SP.800-53r4)


Office of Management and Budget Guidance (OMB):

- Exhibits 53 and 300 – Information Technology and E-Government:
  https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fy14_guidance_on_exhibits_53_and_300.pdf

OMB Circulars:

- OMB Circular A-11, Preparation, Submission, and Execution of the Budget (July 1, 2016):

- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act:

- OMB Circular A-123, Management’s Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016):

- OMB Circular A-130, Management of Federal Information Resources (July 28, 2016):
  https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

OMB Memoranda:

Fiscal Year 2017:

- M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017):
  https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

- M-17-09, Management of Federal High Value Assets (December 9, 2016):
M-17-06, Policies for Federal Agency Public Websites and Digital Services (November 8, 2016):


M-17-02, Precision Medicine Initiative Privacy and Security (October 21, 2016):

Fiscal Year 2016:

M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016):
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf

M-16-17, OMB Circular No. A-123, Management’s Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016):


Fiscal Year 2015:

M-15-14, Management and Oversight of Federal Information Technology (June 10, 2015):

Fiscal Year 2014:


Fiscal Year 2013:


Fiscal Year 2012:


Fiscal Year 2011:


Fiscal Year 2010:

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

• M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010):

• M-10-06, Open Government Directive (December 8, 2009):

**Fiscal Year 2008:**

• M-08-09, New FISMA Privacy Reporting Requirements for FY 2008 (January 18, 2008):
  https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-09.pdf

**Fiscal Year 2006:**

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


  https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-06.pdf

**Fiscal Year 2005:**


**Fiscal Year 2004:**


**Fiscal Year 2003:**


**Fiscal Year 2002:**


• M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones (October 17, 2001): https://obamawhitehouse.archives.gov/omb/memoranda_m02-01/
Fiscal Year 2001:

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

Fiscal Year 2000:

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

Fiscal Year 1999:

- M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999):
  https://www.whitehouse.gov/omb/memoranda_m99-18

  https://obamawhitehouse.archives.gov/omb/memoranda_m99-05/

Fiscal Year 1998:

  https://www.whitehouse.gov/omb/memoranda_m9809
HHS Privacy Policy:

- HHS General Administration Manual, Chapter 45-10, Privacy Act – Basic Requirements and Relationships:

- HHS General Administration Manual, Chapter 45-13, Safeguarding Records Contained in Systems of Records:


- HHS Policy for Section 508 Compliance: [https://www.hhs.gov/web/section-508/index.html](https://www.hhs.gov/web/section-508/index.html)


HHS Cybersecurity Program Privacy Documents:

- HHS OCIO Policies, Standards and Charters
  http://www.hhs.gov/ocio/policy/

- HHS Privacy
  http://intranet.hhs.gov/it/cybersecurity/privacy/index.html

- HHS-OCIO Policy for Information Systems Security and Privacy:
  https://www.hhs.gov/ocio/securityprivacy/index.html

- HHS-OCIO Memo for the Implementation of OMB M-10-22 and 23:
  http://www.hhs.gov/ocio/policy/implementation_of_omb_m-10-22_and_m-10-23.html

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

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

- 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:

- HHS-OCIO-Policy for Machine-Readable Privacy Policies Guide:
  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-OCIO Policy for Managing the Use of Third-Party Websites and Applications:
  http://www.hhs.gov/ocio/policy/policy2013_0001.html

- HHS Updated Departmental Standard for the Definition of Sensitive Information
• HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII):

• HHS Policy for Personal Use of Information Technology (IT) Resources:

• HHS Standard for Encryption of Computing Devices:
  http://intranet.hhs.gov/it/cybersecurity/docs/policies-guides-encryption.pdf

• 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

• Requirements for Role-Based Training of Personnel with Significant Security Responsibilities:
  https://community.max.gov/download/attachments/1205537135/Role-Based%20Training_Memo.pdf?version=1&modificationDate=1499353661193&api=v2
NIH Policy, Provisions & Guidelines:

- NIH Manual Chapter 1754, Reporting Allegations of Criminal Offenses, Misuse of NIH Grant and Contract Funds, or Improper Conduct by an NIH Employee: https://policymanual.nih.gov/1754
- NIH Manual Chapter 1825, Information Collection from the Public: https://policymanual.nih.gov/1825
• NIH Manual Chapter 2805, Web Privacy Policy: 
  https://policymanual.nih.gov/2805

• NIH Manual Chapter 2809, Social and New Media Policy: 
  https://policymanual.nih.gov/2809

• NIH Manual Chapter 3014, Human Research Protection Program: 
  https://policymanual.nih.gov/3014
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

- HHS Privacy Impact Assessment (PIA) Training
  http://intranet.hhs.gov/it/docs/education/privacy_impact/PrivacyImpactAssessmentTraining_20100818_v1.0.pdf

- NIH Privacy and Information Security Awareness Training:
  http://irtsectraining.nih.gov/
Websites:

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

- HHS Cybersecurity Program Online Web Page:  

- 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 OCIO website:  

- NIH OCIO IT Security Policies, Guidelines and Regulations:  
  [https://ocio.nih.gov/InfoSecurity/Policy/Pages/default.aspx](https://ocio.nih.gov/InfoSecurity/Policy/Pages/default.aspx)

- NIH OCIO IT General Rules of Behavior:  

- NIH OCIO Information Systems Security Officers:  

- NIH OCIO ISSO Corner:  
• NIH Privacy Web Page:
  https://oma.od.nih.gov/DMS/Pages/Privacy-Program.aspx

• NIH Privacy SharePoint Website (NIH Employees Only):
  https://oma.nih.gov/dms/programs/privacy/SitePages/Home.aspx

• NIH Records Management Web Page:

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

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

• NIH Privacy Act Systems of Records (SOR) Notices:
  https://oma.od.nih.gov/DMS/Documents/Privacy/Privacy%20Act%20Systems%20of%20
  Records%20Notices%20(SORNs)%205-1-15.pdf

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

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

• NIH Web Authors Group (WAG) Policy & Guidance on Web Site Development,
  Management, and Evaluation:

• NIH Office of Communications & Public Liaison:
  https://www.nih.gov/institutes-nih/nih-office-director/office-communications-public-
  liaison

• NIH OMB Project Clearance:
  http://grants.nih.gov/grants/oer_offices/opera.htm
Other Useful Websites:

- Federal Privacy Council:  
  https://www.fpc.gov/

- OnGuard Online – Your Safety Net:  
  http://onguardonline.gov

- IBM Social Computing Guidelines:  

- US-CERT:  
  http://www.us-cert.gov/

- U.S. Postal Inspection & FBI Funded Website - Looks Too Good To Be True:  
  http://www.lookstoogoodtobetrue.com/index.aspx