Policy Title:	Research Data Security
Responsible Office:	OVPR
Effective Date:	2012
Revision Date:	Fall 2014

INTRODUCTION

Harvard University's Information Security Policy effectively addresses the need to protect confidential and sensitive information that is maintained in the various spheres of University administration. The research setting poses particular information security risks and challenges, including regulatory and contractual constraints that require additional policy provisions and protective measures. While following the Policy Statements of the Harvard Information Security Policy, this policy provides specific guidance for managing research data.

POLICY STATEMENT

Properly protecting research data is a fundamental obligation that is grounded in the values of stewardship, integrity, and commitments to the providers and sources of the data. This policy is particularly focused on the protection of research data that are confidential by reason of applicable law and regulation, agreements covering the acquisition and use of the data, and University policies.

To protect research data appropriately and effectively, the University's researchers, research oversight bodies and Information Security Officers must understand and carry out their responsibilities related to data security. The following security levels, described in the Harvard Data Classification Table, reflect the basic principle that more exacting security requirements must be implemented as the risk associated with the research data increases:

Level 5 - Extremely sensitive information
Level 4 - Very sensitive information
Level 3 – Sensitive, or Confidential information
Level 2 - Benign information to be held confidentially
Level 1 - Non-confidential research information

The Requirements are sets of security controls that correspond to each data security level.

This policy applies to all research data regardless of the storage medium (e.g., disk drive, electronic tape, cartridge, disk, CD, DVD, external drive, paper, fiche, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.), physically housed at Harvard or stored remotely under the management of Harvard researchers.

SCOPE OF POLICY

This Policy applies to researchers and research team members who obtain, access or generate research data, in particular confidential information. The policy applies regardless of the source of funding for the research.

The Policy also applies to the research oversight bodies working with the Office of the Vice Provost for Research, in assisting researchers in identifying and assessing data confidentiality risks; and Information Security Officers working with researchers and research team members to ensure implementation of the security controls for the requirements of the security level designated for research information.

ROLES AND RESPONSIBILITIES

These are the roles and responsibilities of Harvard University researchers (faculty, visiting scholars, post-doctoral fellows, other fellows and students), departments and schools that conduct research and the relevant research oversight bodies, information security officers and sponsored programs offices.

A. Researchers:

Researchers have these responsibilities:

a. Identifying confidentiality and data security obligations, based on laws, regulations, policies, and binding commitments such as data use agreements and participant consent agreements.
b. Except in cases where it is the responsibility of a research oversight body, (see Definitions) it is the responsibility of researchers to identify the appropriate data security level for research data. (See procedures (link) for how to get assistance in setting a data security level.)
c. When the data security level has been established, researchers are responsible for creating and maintaining data documentation, implementing the security controls corresponding to the requirements of the data security level and developing and following a data security plan and procedures over the course of their projects.

B. Information Security Officers:

Local or School Information Security and HUIT Information Security are responsible for assisting researchers with implementation of appropriate security controls in accordance with the level assigned by the Research Oversight Body or specific controls outlined in a DUA. Information Security Officers may be asked to review DUAs for information security controls specified by a data provider. Local or School IT Officers confirm that level 3 checklist requirements have been met, while studies involving Level 4 and Level 5 data require approval by HUIT.

a. ***Variances:*** The Information Security Officer and the Researcher may apply compensating controls for the assigned data security level, if certain controls prescribed for the security level are not feasible. These compensating controls will be documented and attested to by the researcher and the ISO(s), and the ISO will inform the IRB if the project is under IRB review.

b. ***Signature:*** A checklist will not be considered complete without the researcher attestation via signature.

c. ***Facility Certification:*** A research facility may be certified at a certain data security level, enabling projects classified as up to and including that data security level to be exempt from separate review and approval.

C. Research Oversight Bodies:

Research oversight bodies are responsible for:

a. Assessing data security risks associated with the research within their purview and assigning data security levels for the research.
b. Establishing procedures to set security levels, either on a project by project basis, or by category of research data, and
c. Informing researchers about data security risks and working with them to set appropriate data security levels.

While all research oversight bodies share these same basic roles and responsibilities with respect to their engagement with researchers and information security officers, the procedures will vary, depending on the particular research and the oversight body or bodies that may be involved.

D. Office of the Vice Provost for Research

The Office of the Vice Provost for Research is responsible for:

a. Implementing this policy
b. Working with research oversight bodies to identify data security risks and set data security levels, and
c. Working with researchers and IT and HUIT as appropriate, to foster awareness and understanding of the policy.
d. Periodically reviewing adherence to the policy

PROCEDURES

Procedures to implement this policy will be developed and maintained by the Office of the Vice Provost for Research, in consultation with the Office of the University Chief Information Security Officer and research oversight bodies as appropriate.

Identifying and Assessing Security Risks and Implementing Security on a Project by Project Basis

Researchers who plan to use data that are confidential, but do not fall in one of the categories

described below, should select a security level from the Data Classification Table that is appropriate for the nature of the data, and implement the security controls for that level. Questions about selecting a security level can be directed to any of the Research Oversight Bodies or Research Data Security Help, RDSAP@harvard.edu. Questions about implementing security controls can be directed to a School Information Security Officer, HUIT or Research Data Security Help, RDSAP@harvard.edu

1. Use of data about persons:
    a. Human subjects research, during IRB review and approval
    b. Research involving data from individuals, not reviewed and approved by an IRB
2. Data use agreements containing data security requirements
3. Laboratory Animal Care and Use (Animals covered by IACUC policy)
4. Commercial or Program Data
5. Technical data under ITAR and other data with export controls – based data security requirements
6. Select agents
7. Genomic data
8. Intellectual property

1. *Use of data about persons*

One major category of research involving data about individuals is "human subjects research", which is reviewed and approved by IRBs. In order for IRBs to approve research they must conclude that adequate provisions have been made for protecting the privacy of subjects and the confidentiality of personal information. Accordingly, it is the responsibility of IRBs to specify the security level for research projects they review and approve, and to obtain confirmation that the relevant security controls are being implemented. The research data security procedures, carried out in conjunction with IRB review and approval, are set out in Section A below.

The research data security procedures for research projects that involve data about individuals that are not reviewed and approved by an IRB are set out in Section B.

A. Human Subjects Research, during IRB review and approval

1. When applying for IRB approval, the researcher will describe the subjects to be recruited, any personally identifiable information that will be acquired, how the information will be collected, the number of subjects, promises or representations regarding confidentiality made to subjects in recruitment materials and consent forms, and measures to protect the confidentiality of information, such as maintaining a key code or physical security provisions for paper records.
2. The IRB will consult with the researcher, obtain additional information as needed, assign a security level to the project based on the sensitivity of the data, and direct the researcher to the Requirements checklist for the data security level (see Related Documents).
    2.1. DUAs may dictate additional security measures, which will be evaluated by the IT Security team. See Data Use Agreements section for more details

3. For projects designated data classification level 3, the IRB will complete its review and grant final approval. As outlined in the IRB approval letter, the researcher must meet the security requirements, and return the signed checklist to the IRB by the study's continuing review.
4. For projects designated data classification level 4, or 5, the IRB will complete its approval process upon receipt of the signed checklist from the researcher.
5. Submitting Data Security Attestation
   5.1. For projects designated data classification level 1 or 2, researchers can implement the security controls set out in the Requirements checklist without contacting Local or School IT or HUIT, though those offices are ready to provide assistance if asked.
   5.2. For projects designated data classification level 3, the researcher should consult with Local or School IT or HUIT Information Security in order to implement the security level controls for the requirements of the security level. When the researcher has met physical, network, and system security controls for the requirements of the security level, and documented and put in place required operational procedures, the researcher must submit a signed checklist to the IRB.
   5.3. For projects designated data classification level 4 or 5, the researcher must consult with HUIT Information Security in order to implement the security level controls for the requirements of the security level. When the researcher has met physical, network, and system security controls for the requirements of the security level, and documented and put in place required operational procedures, the researcher must submit a signed checklist to the IRB.

B. Research involving data from individuals, not reviewed and approved by an IRB

These procedures cover two types of research projects: ones that have been determined to be either "exempt" or "not human subjects research" by an IRB, or ones that a researcher has independently determined to be "not human subjects research" (under IRB policy, researchers may not decide on their own that their projects are "exempt").

1. When an IRB has deemed a project "exempt" or "not human subjects research"
   a. Where possible based on the materials submitted by the researcher, the IRB should propose, but not mandate, a security level for an "exempt" or "not human subjects research" project, direct the researcher to the security requirements for that level, and inform the researcher of the availability of assistance from the local or School Information Security Officer or HUIT to implement those controls.
   b. At the request of a researcher, the local or School Information Security Officer or HUIT will provide assistance in implementing the security controls for the security level.
2. Research projects involving data from individuals, that have not been submitted to an IRB, where the researcher identifies confidentiality or privacy concerns
   a. A researcher who plans a research project that is not "human subjects research," but could potentially raise privacy or confidentiality concerns, is advised to enlist the assistance of the IRB, or the Research Data help desk at rdsap@harvard.edu, in assessing the risk, and the assistance of Local or School Information Security or HUIT to implement measures to reduce the risk.

2. ***Data Use Agreements (DUAs)***

Data Use Agreements[1] (DUAs)

Parties who provide researchers with data sets may impose restrictive publication or use terms and/or additional data security controls through DUAs. Once a Researcher receives a DUA from a data provider, he or she should submit the DUA, along with a description of the proposed research to:

a. Their relevant IRB If the research involves data about persons
b. Their relevant sponsored programs office.
c. Their Local or School Information Security Officer or HUIT Information Security at **ithelp@harvard.edu**.

Review: Concurrent with the OSP/SPA review and negotiation process, the Information Security Officer will work with the Researcher to review the security requirements of the DUA to determine whether any specific protections need to be employed to meet the requirements of the data-provider.

***Certification*:** When the Information Security Officer is satisfied that the Researcher's proposed plan for securing the data meets the requirements of the data-provider, the School data security expert will forward the DUA and other documents (e.g. Data Request and IRB approval, if applicable) to the relevant OSP/SPA with a cover note or email indicating approval and advising that the physical and computing security controls in the DUA can be met. If the agreement requires institutional signature OSP/SPA will provide the signature; if no institutional signature is required the agreement will be returned for local school or department to arrange for signature of the DUA within the school or department's discretion.

See the DUA Guidelines for additional information on DUAs <*link forthcoming*>.

3. Laboratory Animal Care and Use (Animals covered by IACUC policy)

The *Guide for the Care and Use of Laboratory Animals* identifies two areas of risk management that include data security protection, and are applicable to researchers[2]:

1. Medical Evaluation and Preventive Medicine for Personnel, implicating personal health information, and
2. Personnel Security calling for "physical and information technology security" to protect against "threats that criminal activities such as personnel harassment and assault, facility trespassing, arson and vandalism pose to laboratory animals, research personnel, equipment and facilities."

Researchers whose projects include laboratory animal studies should:

[1] See definitions: Terms of data use can be included in many different types of agreements
[2] For more specific information contact the IACUC committee or review the NIH information at http://grants.nih.gov/grants/policy/air/preparedness_help.htm

1. Consult with their IACUC committee to assist them in identifying categories of laboratory information that require secure storage and use, and the appropriate security levels for that information, and
2. Consult with their Local or School Information Security Officer for assistance in implementing the applicable security measures.

4. *Commercial or Program Data*

Organizations including corporations, governmental bodies, and non-profit entities frequently provide data to researchers that may be sensitive for reasons such as financial or reputational risk to the organization. ***[Note: organizations may provide personal information in their possession. Unless all direct and indirect identifiers have been removed by the organization, researchers are advised to contact their IRB before receiving and using such data.]***

When organizations provide sensitive data without a formal DUA, researchers should:

1. Evaluate the sensitivity of the data,
2. Review the Data Classification Table and related guidance materials and select the data security level that best describes the data, and
3. Implement the security controls of the Requirements for the data security level, with the assistance of Local or School Information Security Officers or HUIT as appropriate.

5. Data Subject to Export Controls

In general, it is safe to assume that, if an item or technology is subject to export controls, the data related to the item or technology is also subject to export control. Researchers who think their projects may be subject to export control regulation should:

1. Consult with their School's representative on the Export Control Council to identify any data security obligations that are associated with export control requirements, and
2. Consult the Export Control Guidance for Outsourcing Information Technology Services when seeking to outsource information technology services.
3. Consult with their Local or School Information Security Officer for assistance in implementing the applicable security controls.

See the HRDSP FAQs for additional information about data security issues associated with data related to items or technology subject to export controls.

6. ***Biosafety: Select Agents and Toxins***

Data security measures are necessary to protect against the release of data that would allow an unauthorized individual to gain access to select agents or toxins. The Committee on Microbiological Safety (COMS) reviews research that presents biohazard risks, including research that involves biological toxins subject to the Federal Select Agent Program.

Researchers who work with infectious agents or other biohazardous material should:

1. Consult with COMS to assist them in identifying categories of laboratory information that require secure storage and use, and the appropriate security levels for that information, and

2. Consult with their Local or School Information Security Officer for assistance in implementing the applicable security controls.

7. ***Genomic Data***

A data sharing plan may be necessary for the sharing and accessing of genomic data. Researchers seeking to share or access genomic data from NIH's dbGaP repository should: Consult with their local IRB before depositing genomic data into dbGaP.

8. ***Intellectual Property***

Research may lead to the discovery of inventions for which patent applications should be prepared. In most cases, the prospect of such inventions should not require heightening data security levels: the basic measures that are expected of all researchers consistent with the practice of good stewardship will provide adequate protection.

Researchers who have particular concerns about the data security aspects of protecting inventions so they may be patented should contact the Office of Technology Development,

Setting and Implementing a Security Certification at a Facility, School or Lab

1. Facility Certification

A facility that has been approved by Local or School Information Security Officer or HUIT Information Security for a research project that has been assigned Security Level 3, 4, or 5, may be certified by Local or School Information Security Officer or HUIT Information Security for use on research projects having the same or lower Security Level. Individual research plans that are identified as having data that require a security level greater than the level of the facility certification will need additional controls that are reviewed and approved by HUIT.

Certification of Level 4 and 5 facilities requires final review and approval by HUIT.

In order for a facility to be certified, the following steps must be carried out in addition to the initial Security Level approval by Local or School Information Security Officer or HUIT Information Security:

1. Designation of a facility manager who will:
    a. Maintain a file of active projects storing data on the facility servers or computers,
    b. Be responsible for carrying out operating procedures specified in the relevant Security Level checklist,
    c. Ensure that researchers who store data at the facility are informed of their responsibilities, as set forth in the relevant Security Level checklist, and that the researchers acknowledge those responsibilities
2. Notification by Local or School Information Security Officer or HUIT Information Security of facility certification, to the researcher, the researcher's department, and the IRB, of the date of facility certification and the period of certification, which should not exceed one year.

Renewal: HUIT will notify the designated facility manager before the end of the period of certification. If the facility needs its certification renewed in order to support ongoing or anticipated future projects, HUIT and the facility manager will confer and establish a review plan for the renewal. Upon renewal, notification will be carried out as with original certification, see preceding paragraph.

Definitions

Data Use Agreement: Any agreement between a data provider and a researcher who requests the data concerning access to and the transfer, use, security, or disposal of the data. DUAs are not limited to agreements specifically identified as such and may include License Agreements, Confidentiality Agreements, Non-Disclosure Agreements, Memorandums of Understanding, Memorandums of Agreement and other agreements under other names that include terms and conditions governing access to and the transfer, use, security and disposal of a pre-existing third-party owned data set.

Facility: Any computer, computer network, or cloud computing environment and the office or laboratory in which it is situated, or from which it is managed, used for the processing and/or storage of research data.

Facility Certification: Approval of a facility for processing and storing research data of a specified security level, either level 3, 4, or 5, by HUIT or IT, so that approval does not have to be obtained on a protocol-by-protocol basis.

Harvard Information Security Policy: The Harvard University Policy that covers all administrative data.

Harvard Research Data Security Policy [HRDSP]: The Harvard University Policy that covers all research related data, regardless of format or funding.

HUIT Information Security [HUIT]: The Harvard University Security Information Office, see http://security.harvard.edu

Human Subjects Research: As defined in the Common Rule, 45 CFR 46 §102: research that involves obtaining data about a living individual through intervention or interaction with the individual, or obtaining identifiable private information about the individual.

IRB: Institutional Review Board, a committee that performs ethical review of research involving human subjects. Harvard has three IRBs, see details in "Contacts and Subject Matter Experts" below.

Personally Identifiable Information (PII): Refers to information that identifies, or can be used to identify an individual, either alone or when combined with other personal or publicly available information that

is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for a researcher or oversight body to recognize that additional sources of information, not known or anticipated at the time of their assessment, may become publicly available, enabling identification of individuals in data sets that had previously been considered free of PII.

Private information: includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). (Level 3, 4, or 5)

Protected Personally Identifiable Information: an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. A similar definition is found in the Massachusetts regulations protecting personal information, referred to in Harvard data security policies and procedures as High Risk Confidential Information (HRCI), and, with respect to medical information, in the HIPAA Privacy Act, referred to as Protected Health Information (PHI). (level 3, 4, or 5)

Research Oversight Body: A committee, council, office or other unit that has some responsibility for promoting awareness of, and compliance with, laws, regulations or policies that apply to research-related activities. Examples include IRBs, the Office for Sponsored Programs (OSP), the Export Control Council, and the Committee on Microbiological Safety (COMS).

Researcher: Any investigator (e.g. Faculty, student, post doc, etc) who seeks to obtain research data from a third party, or conducts research where data are generated or used.

School Information Security Office [IT]: The designated Security Information Officer at a School, or the Chief Information Officer of the School.

Security Control: A safeguard measure to reduce a risk of data breach. There are sets of security controls that are required for each Security Level of the Data Classification Table.

Security Level: The assigned information risk designation for a research project, on the Data Classification Table. For human subjects research projects the IRB assigns the security level, in consultation with the researcher and IT or HUIT as appropriate. Security levels should be designated for confidential research data that does not involve human subjects by the researcher in consultation with the research oversight body as appropriate, as set forth in the Procedures implementing this policy.

Related Resources, Documents and Policies

Data Classification Table

Security Level Checklists

Data Use Agreement Guidance ***[pending]***

ADAMS Information Security and Data Use Agreement approval and tracking system: https://adams.harvard.edu

DUA Templates developed by OSP (being updated)
- Non PHI incoming Data
- PHI Incoming Data
- Non PHI Outgoing Data

Policy on Access to Electronic Information

Information Security Policy/Charter

Acceptable use of Information Resources

Electronic Data Security Breach Reporting

IT Vendor Assessments

Disposal of Electronic Information

Backup of Electronic Information

Harvard University Policy on Publications at: http://osp.fad.harvard.edu/content/policy-publications

Select Agents Information Systems Security Control Guidance

Contacts and Subject Matter Experts

Research Data Security Help email: RDSAP@harvard.edu

The Office of the Vice Provost for Research: http:///www.vpr.harvard.edu

School Information Security Officers

The Office for Sponsored Programs; Grants and Contracts Officers, Sponsored Program Officers & Team Managers.
Full contact list available at: http://vpf-web.harvard.edu/osp/pdfs/Website-Contacts.pdf

The Office of Technology Development: http://www.otd.harvard.edu

HMS/SPA: http://www.hms.harvard.edu/spa/index.shtml

HSPH/OFS: http://www.hsph.harvard.edu/administrative-offices/financial-services/index.html

Office of the General Counsel: http://ogc.harvard.edu/

Institutional Review Boards

Harvard School of Public Health: Institutional Review Board

Harvard University Faculty of Medicine: Institutional Review Board

Contact and location information:

- Phone: 617-432-2157
- Fax: 617-432-2165
- Email: irb@hsph.harvard.edu
- Website:
  - HSPH: www.hsph.harvard.edu/ohra
  - HMS/HSDM: www.hms.harvard.edu/ohra
- Address:
  Office of Human Research Administration
  Harvard Longwood Medical Area
  90 Smith Street
  3rd Floor-Room 335
  Boston, MA 02120

University Area: Committee on the Use of Human Subjects (CUHS)

Contact and location information for the Committee on the Use of Human Subjects:

- Phone: 617- 496-CUHS
- Fax: 617-496-7400
- Email: cuhs@fas.harvard.edu
- Address:
  Harvard University
  1414 Massachusetts Avenue, Second Floor
  Cambridge, MA 02138