The use and categorization of research information at Harvard

Introduction

This memo discusses the protection of research information at Harvard. The office of the University Technology Security Officer (UTSO), working with the Vice Provost for Research, the IRBs, Risk Management and Audit Services, and the OGC, has established information security categories, or levels, and accompanying sets of measures to protect research information: the higher the security category, the more exacting the protective measures, which are based on the standards of the Harvard Enterprise Security Policy for protection of comparable confidential information throughout the University. These categories and related protection requirements are described in the Harvard Research Data Security Policy (HRDSP) which can be found on the University security website. While the responsibility for protecting confidential data ultimately rests with researchers, the University provides the following guidance and support.

The Security Information Officer and the Chief Information Officer of each School (IT), working with the University Technology Security Information Officer, are available to review and approve researchers’ information security arrangements. In the case of human subjects research, the Institutional Review Boards (IRBs) review study data security plans to ensure the protection of confidential information of research participants.

In the case of human subjects research, the following groups have specific responsibilities under the research security policies:

1. Investigators are responsible for: disclosing the nature of the confidential data they collect so the IRB can assess the data security risk; preparing study data security plans and procedures in accordance with the appropriate security category requirements; and for implementing and monitoring the data security plans and procedures over the course of their projects.

2. The IRBs are responsible for ensuring the adequacy of Investigators’ provisions to maintain the confidentiality of data in human subject research. The IRB fulfills its responsibility by obtaining the assurance of the investigator that the Harvard Research Data Security Policy (HRDSP) requirements for the applicable security category will be followed. The IRB may approve variances from the security requirements that would apply to a study given its security category, so long as the resulting study data security plan complies with any legal requirements. The IRBs may seek the advice and recommendations of IT and the UTSO in assessing the adequacy of provisions to maintain confidentiality of data and in approving a data security category level.

3. IT will be responsible for assisting investigators and IRBs to identify the security categories appropriate for studies, as necessary, and for assisting investigators to implement the appropriate security requirements for their studies.

A research facility may receive the UTSO’s or a School security information officer’s written designation that it meets the requirements of an information security category, subject to annual
review. A copy of that designation may be submitted by the researcher to the IRB to satisfy the research information security requirements of projects utilizing the approved facility.

1.0 Research Information from Non-Harvard Sources

Some research information in use at Harvard comes from non-Harvard sources or is the result of research by Harvard personnel in non-Harvard facilities.

Research information from non-Harvard sources is often accompanied by a use agreement (such as a data use or business agreement) that defines use limitations and/or protection requirements for the information. Harvard personnel working with such research information must, at a minimum, comply with the use limits and protection requirements in the use agreement. If confidential information is subject to security requirements specified in an information use agreement, grant, or contract, those requirements must be met. If a Harvard researcher will obtain information about human subjects, see 2.0 below, IRB review and approval is required.

Harvard personnel using non-Harvard facilities, such as hospitals, are usually subject to the security policies in force at such facilities, as is the research information collected using such facilities. Note that the research may be covered by the policies of both Harvard and the non-Harvard facility. In the event that the non-Harvard facility lacks an applicable policy, the research information should be protected under Harvard policies.

Note that individual researchers do not have the authority to sign an information use agreement on behalf of the University. Only offices that have been specifically authorized may sign such agreements, even when the agreements do not include any transfers of funds. Authorized offices are the University Office for Sponsored Programs, the Medical Area Sponsored Programs Administration, the School of Public Health Sponsored Programs Administration, and the Office for Technology Development. (See the Research Data Protection process document on http://www.security.harvard.edu/resources/forms for more information.)

2.0 Research Information from Harvard Sources

Research. Federal regulation 45 CFR 46 defines research as “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.”

Human Subjects. Federal regulation 45 CFR 46 defines a human subject as “a living individual about whom an investigator (whether professional or student) conducting research obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information. Under these regulations and Harvard University policy, all "human subjects research" at Harvard must be reviewed by an IRB before any related research activities are conducted. Personally identifiable information collected for, used in, or resulting from research involving human subjects must be protected from inadvertent or inappropriate disclosure. The IRBs will confirm the security level categorization and the researcher’s assurance that security requirements are satisfied. In conducting its review, IRB may rely on the attestation of the researcher, may request confirmation that there has been a satisfactory information security office
Other Sensitive Research. Harvard researchers often deal with sensitive information that does not relate to human subjects. This information can include proprietary information subject to confidentiality requirements, and information with national security implications. Most of these types of information should be categorized as Level 3 information under the categories described below. However, information with national security implications generally will be categorized as Level 4 information. Researchers should consult with their school IT groups to determine the proper level for these types of information if they are not sure how to categorize it.

3.0 Information Security Categories

Harvard information security has specific security requirements for research information in each of the following categories:

**Level 5 - Extremely sensitive information about individually identifiable people**

Level 5 information includes individually identifiable information that could cause significant harm to an individual if exposed, including, but not limited to, serious risk of criminal liability, serious psychological harm or other significant injury, loss of insurability or employability, or significant social harm to an individual or group.

**Level 4 - Very sensitive information about individually identifiable people**

Level 4 information includes individually identifiable High Risk Confidential Information (HRCI) as defined by the Harvard Enterprise Information Security Policy. This includes Social Security numbers as well as other individually identifiable financial information. (See http://www.security.harvard.edu/enterprise-security-policy/1-high-risk-info for a full list.) Medical records that are not categorized as extremely sensitive and other individually identifiable research information that, if disclosed, could reasonably be expected to present a non-minimal risk of civil liability, moderate psychological harm, or material social harm to individuals or groups should also be classified as Level 4 information. Medical records may also be subject to Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. Subject to specific government requirements in each case, sensitive national security information should usually be classified as Level 4 information.

**Level 3 - Sensitive information about individually identifiable people**

Level 3 information includes individually identifiable information that, if disclosed, could reasonably be expected to be damaging to a person's reputation or to cause embarrassment. Student record information protected by FERPA also generally falls under Level 3.

**Level 2 - Benign information about individually identifiable people**

Level 2 information includes individually identifiable information, disclosure of which would not ordinarily be expected to result in material harm, but as to which a subject has been promised confidentiality.
Level 1 - De-identified research information about people and other non-confidential research information

Research information in which all information that could be used, directly or indirectly, to identify an individual has been removed or modified is referred to as "de-identified research information," described in Federal IRB regulations as information “recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects.” The HIPAA Privacy Rule for protected health information specifies eighteen categories of information that must be removed in order to de-identify data. There are no specific University requirements for the protection of de-identified research information or for other non-confidential research information, but researchers may want to protect such data for their own reasons, i.e., keeping data private until a paper about the data is published.

4.0 Legal Requests for Research Information

On occasion, a researcher will receive a subpoena, national security request or court order demanding disclosure of information in their possession. Should this occur, the researcher must tell the person making the request to contact the Office of the General Counsel (Office Administrator: 617-495-3006). No one at Harvard, other than the Office of the General Counsel, is authorized to respond to these types of requests. (See http://www.hks.harvard.edu/research/FOIAmemo11-29-99-1.doc for information on responding to FOIA requests.)

To guard against the compelled disclosure of research data containing individually identifiable information, researchers should consider obtaining applicable government-provided protections for the data. For example, research may qualify, upon application, for a Certificate of Confidentiality. A Certificate of Confidentiality will allow a researcher to refuse to disclose personally identifiable information concerning research subjects in civil, criminal, administrative, legislative or other proceedings. Such subjects can be protected if the research information could damage their financial standing, employability, insurability or reputation. Certificates of Confidentiality can be obtained from the NIH for NIH funded research. (See http://grants2.nih.gov/grants/policy/coc/ for more information.) The Department of Justice also may grant similar protections, upon application, for research involving criminal records. Research funded by the Agency for Health Care Policy and Research enjoys a form of automatic protection. Investigators should consult their IRB office for further information on obtaining these protections.

Effective date October 7, 2010