Stanford University Policy

Departing Personnel Data Management and Access

I. POLICY STATEMENT

Stanford University recognizes the importance of 1) its legal, ethical and contractual stewardship obligations in maintaining the security and integrity of High Risk data, and the privacy of individuals, such as research subjects, patients, employees, and students; 2) its Openness in Research principles, including the desire for departing personnel to have continuing access to certain research data; and, 3) preserving institutional assets, such as documents and data supporting Stanford operations.

II. PURPOSE

This policy specifies the appropriate disposition of Stanford High Risk Data in the possession of any departing member of the Stanford Community.

III. APPLICABILITY

Who: All members of the Stanford University Community ("Person" or "Personnel"), including faculty, staff, students, scholars, fellows, and residents; observers and visitors when they are doing business with Stanford; individuals who volunteer or otherwise assert an association with the University; and Contractors.

What: All Stanford High Risk Data (defined below). Hospital data is also subject to Hospital policies.

When: All situations involving Departing Personnel. This policy does not currently apply to leaves of any kind.

IV. KEY TEMS AND DEFINITIONS

Contractor: Vendors, consultants, collaborators, subrecipients or any other entity not affiliated with Stanford.

Data Governance Board ("DGB"): University panel consisting of representatives from the Privacy Office, Information Security Office, and the Office of General Counsel.

Depart/ing/ure: Disaffiliation of any kind with Stanford, including retirement, resignation, termination, graduation, transfer to another institution, or completion of a fixed-term appointment or contract.

Low Risk, Moderate Risk, and High Risk: Classifications of Stanford Data, as defined by the Stanford Risk Classifications found at dataclass.stanford.edu.

Stanford: Stanford University. This excludes the Hospitals, Clinics, University Healthcare Alliance ("UHA") and the Lucile Packard Healthcare Alliance ("PCHA").

Stanford Data/Data: Any recorded information generated, obtained, recorded, or stored at Stanford, in systems or facilities under Stanford's control or under custody or management of Stanford Personnel. Such information includes technical, health, student, employee, operational or business information; data that is identifiable or de-identified, individual or aggregated; and, information stored in paper files, personal devices, databases, and systems.

V. OWNERSHIP OF DATA

Personnel do not gain an ownership interest in or title to any Stanford Data for projects or work conducted at Stanford or with Stanford resources. Ownership and use of patient, employee, student, and research data are governed by applicable laws and regulations, sponsor requirements, and contractual obligations.

VI. POLICY AND RESPONSIBLE PARTIES

A. Departing Person

1. No later than five business days prior to Departure, each Departing Person shall complete and electronically sign the Departing Personnel Data Disposition Form, found on the Privacy Office website (privacy.stanford.edu). If the Departure is a result of termination, the Departing Person shall complete the form at the time of termination.
2. For continued access to Stanford High Risk Data or systems containing such High Risk Data, the Departing Person shall complete the online request portion of the Departing Personnel Data Disposition Form, found on the Privacy Office website, no later than five business days prior to Departure. ***Contractors may not continue to access Stanford Data or systems, regardless of the Risk Classification.***

B. Departing Person's Supervisor, Faculty Advisor, or Department Chair (Manager)

1. The Departing Person's Manager shall be responsible for ensuring that the Departing Person is informed of this Policy and arranging for the Departing Person to complete the appropriate form(s).
2. In the event that a Departing Person's Manager learns that a Departing Person failed to complete the form(s) or completed the form(s) inaccurately, the Manager shall promptly notify the Privacy Office and assist the Privacy Office in addressing any concerns.

C. Departmental Human Resources, Faculty Affairs or Student Affairs Office (Administrative Offices)

1. As part of its off-boarding process, the cognizant Administrative Office shall require Departing Personnel to complete the Data Disposition Checklist and Attestation Form and, if applicable, the Request for Continued Access to High Risk Data Form prior to Departure, or in the case of termination, at the time of Departure.
2. The cognizant Administrative Office shall seek guidance from the University Privacy Office regarding special departure cases, such as extended leave, sabbatical, or leave outside the United States, where the individual requests access to Stanford High Risk Data.

D. University Privacy Office

1. The Privacy Office will maintain this policy and monitor its implementation across Stanford for compliance and consistent application.
2. The Privacy Office will maintain the Data Disposition Checklist and Attestation Form and the Request for Continued Access to High Risk Data Form and make them available for electronic completion on its website.
3. The Privacy Office will maintain the completed forms and periodically monitor the attestations for reasonableness given the Departing Person's roles and responsibilities.
4. The Privacy Office will review all requests for continued access to Stanford High Risk Data or systems that handle High Risk Data, and will work with the DGB to evaluate the request and obtain approval, if appropriate.
    a. If approved, the Privacy Office will notify the Departing Person and the relevant Administrative Office that all steps are completed.
    b. If not approved, the Privacy Office will:
        i. Notify the Departing Person and determine if there is additional information that should be considered, and present any new information to the DGB for consideration.
        ii. Notify the Departing Person and the relevant Administrative Office of the DGB decision.
5. The Privacy Office shall conduct fact-specific reviews and provide guidance regarding special departure cases, such as extended leave, sabbatical, or leave outside the United States, where the individual requests access to Stanford High Risk Data.

E. Data Governance Board

The DGB shall review all requests for continued access to Stanford High Risk Data or systems that handle High Risk Data and collaborate with the appropriate administrative offices to consider such requests.

VII. DATA UPON DEPARTURE

A. Original Records

Departing Personnel may not remove original records of any Stanford Data, regardless of the Risk Classification. All original records of Data and all administrative access rights to such Data, will be retained by Stanford, even after the Person leaves.

B. High Risk Data

1. Protected Health Information ("PHI")

a. Departing Personnel may not retain, access, use, process, transfer or take any copies, iterations, notes, records or files of any PHI, even if access privileges have not been revoked or if the Stanford Data was stored on the Person's personal device, except pursuant to Section VI and Appendix A of this Policy.

b. Departing Personnel shall also review and comply with the Data policies of the Hospital for PHI, as applicable.

2. High Risk Data other than PHI

Departing Personnel may not retain, access, use, process, transfer or take any copies, iterations, notes, records or files of any Stanford High Risk Data, even if access privileges have not been revoked or if the Stanford Data was stored on a personal device, without written approval from the DGB, per Section VI of this Policy.

VIII. CONSEQUENCES OF NON-COMPLIANCE WITH POLICY

The Stanford Community is expected to act in strict accordance with this policy, as the consequences of non-compliance may be severe. Non-compliance may lead to severe consequences for the Departing Person, including federal and state penalties, debarment, fines or criminal penalties, lawsuits, and disciplinary actions.

IX. RELATED DOCUMENTS, FORMS AND TOOLS

Departing Personnel Data Disposition Form
Stanford Risk Classifications
Privacy Office website
Manage Your Research Data
Research Policy Handbook
HIPAA Privacy Rule Minimum Necessary Standard

X. REVIEW AND REVISION HISTORY

- AUGUST 2016 (Version 1.0)

This policy and procedures document will be reviewed, and updated as appropriately, at least every two years, or more frequently if the underlying laws and regulations change.

XI. CONTACT FOR QUESTIONS RELATED TO THIS POLICY

Stanford University Privacy Office
privacy@stanford.edu
(650) 725-1828

APPENDIX A

Specific Policies for Research Protected Health Information (PHI)

1. Departing Personnel and Contractors may not retain, access, use, process, transfer or take any copies, iterations, notes, records or files of any PHI, even if access privileges have not been revoked or if the Stanford Data was stored on the Person's personal device, except as noted below or pursuant to an appropriately executed contract between Stanford and the Departing Person's new institution.
2. The HIPAA privacy regulations and California law continue to apply to all PHI, even after Personnel leave Stanford. PHI may be subject to Hospital data policies. In that instance, the Departing Person may have obligations under the Hospital policies, policy as well as this policy. If the protocol provides for use of or access to Hospital systems or Hospital PHI, the Departing Person will be subject to all Hospital security and privacy policies and procedures.
3. In some instances, a member of the research team leaves Stanford but needs to continue working with study Data for a limited period and for certain purposes, such as to complete data analysis or a publication ("limited continuing purpose"). In this case, if the Departing Person is the Protocol Director ("PD") listed on the IRB protocol application, PD responsibilities shall be relinquished to a current PI-eligible Stanford faculty member who will be responsible for ensuring continued adherence to privacy and security requirements for all study Data. The Departing Person and/or the Protocol Director is required to notify the IRB of the transition in advance and modify the protocol if the IRB deems appropriate. The following criteria and process are required to be met for the IRB to consider approval in a specific study:
    a. The Departing Person is required to have previously been part of the Stanford HIPAA workforce (e.g., as a faculty member or trainee in the Stanford Affiliated Covered Entity).
    b. The study shall remain under the Stanford IRB's oversight.
    c. The Departing Person may only use the PHI solely for an approved limited continuing purpose (described by the PD) as part of the Stanford study; this purpose may not include any interaction with subjects (e.g., for enrollment, consent, or study procedure purposes).
    d. The Departing Person may only conduct the work in an individual capacity (the work shall not be conducted as a member of the new institution, and the researcher may not share the PHI with any other person outside of the Stanford research team).
    e. The PD shall ensure de-identification of the Data whenever possible for the limited continuing purpose; otherwise, if PHI is involved, the PD shall determine if a Limited Data Set would suffice for the limited continuing purpose.

f. If neither de-identified Data nor a Limited Data Set allows completion of the limited continuing purpose, the PD will determine the minimum necessary Data needed for the limited continuing purpose. The PD and Departing Person will arrange for secure ongoing access to the Data through the School of Medicine's Information Resources & Technology ("IRT") and obtain approval of the security plan from IRT and the Privacy Office. The PD and Departing Person will execute a Secure Data Access/Use Plan & Confidentiality Agreement, which ensures continued protection of the Data during the limited period and includes a plan for return and/or secure destruction of the Data as soon as the limited continuing purpose is completed, or earlier at Stanford's discretion. Prior to the IRB's consideration, the PD will provide the executed Secure Data Access/Use Plan & Confidentiality Agreement to the IRB.

g. In this instance, the Departing Person remains subject to all Stanford HIPAA Workforce policies, procedures, and related requirements, including but not limited to timely updating required attestations and completing annual HIPAA trainings. To the extent the Departing Person remains part of the Stanford HIPAA Workforce and subject to the Stanford IRB's oversight for the approved study, the Data use will be considered an internal use of PHI. Upon completion of the limited continuing purpose or earlier as indicated above, the Departing Person will no longer be part of the Stanford HIPAA Workforce.

h. In any study requiring consent/HIPAA authorization, in which a researcher reasonably believes they may leave Stanford before the research is complete and ongoing PHI access may be needed, the consent/HIPAA authorization shall provide for that situation.

i. In the event of a breach or suspected security/privacy incident involving the Data, the researcher shall immediately report the incident to the IRB and to the University Privacy Office and shall fully cooperate with the investigation, mitigation, and other actions.