Research Data Management & Compliance

Rachel Talentino
Research Compliance Officer
Office of the Vice Provost for Research
What will be covered?

The Harvard Research Data Security Policy (HRDSP) focuses on management of Research Data, inclusive of:

- human subjects research data,
- data subject to foreign, federal or state regulations,
- data exchanged pursuant to a data use agreement (DUA), and
- data subject to sponsor requirements or intellectual property protections
The HRDSP also mandates use of three applications in the Compliance System:

- **Research Data Safety & Security Application (Safety Application):** supports research data security plan review by Information Security Reviewers (“Security Review”)
- **ESTR-IRB Application (ES**TR):** support human subjects research reviews by the IRBs (“IRB Review”)
- **Agreements-DUA Application (Agreements Application):** supports data use agreement (DUA) reviews by the Negotiating Offices (“DUA Review”)
What is Research Data?

- Resulting from projects conducted at the University/on Harvard property
  - Ex.s: In your lab, office, classroom, etc.

- Developed or collected under the auspices of the University, even if research activities are occurring elsewhere
  - Ex.s: Interviewing study participants in Europe, data co-developed at collaborator institution

- Developed or collected with University resources (equipment, funding, etc.)
  - Ex.s: Sponsored or internal seed funding, using a HU telescope or air censors developed in a HU lab

For full definition, go to Research Data Retention Policy
IRB Review & “Sensitive” or “Non-Sensitive” determination
The Harvard University Area (HUA) IRB & Longwood Campus IRBs review projects containing “research involving human subjects”

- Requests for IRB review should be submitted in the ESTR application
- Based on the information and documentation submitted in ESTR, the IRB administrator will determine if the study is Sensitive or Non-sensitive (historically would apply Data Security Level (“DSL”))
- If Sensitive → required to submit request for Security Review in the Safety Application and Manage Related Projects
What is Sensitive Research Data?

As I mentioned earlier, Sensitive Data must be submitted in the Safety Application for Security Review!

Sensitive Research Data is historically Data Security Level 3, 4 or 5 -

For example:

- Data subject to Foreign, Federal or State regulations, including GDPR
- “Confidential” data: information that could cause risk of material harm if disclosed
- “High Risk Confidential” data: information that would likely cause serious harm if disclosed
- “Extreme Risk” data - information that would cause severe harm if disclosed
Quick Takeaways!

- IRB makes “Sensitive” or “Non-Sensitive” determination
- “Sensitive” data aligns with DSL 3-5, “Non-sensitive” aligns with DSL 1-2
- Studies that receive a “Sensitive” determination must also be submitted in the Safety Application for Security Review
Data Security Level
1-5 Research Data
What if IRB review is not required?

The faculty member managing or supervising the project must determine the DSL based on Enterprise Policy (and HUIT’s new research-specific examples!):

- **DSL1** - Publicly available and unrestricted data
- **DSL2** - Unpublished non-sensitive research data, whether identifiable or not. Active research data at Harvard is at least DSL2 until published

**DSL 1 & 2 do not require Security Review!**
What if IRB review is not required?

DSL 3-5 do require Security Review in the Safety Application!

- **DSL3 - Sensitive Data**: Some regulated data, or data that could be damaging to the subject’s financial standing, career or economic prospects, personal relationships, insurability, reputation, or be stigmatizing.

- **DSL4 - Sensitive Data**: Data that could place the subject at risk of significant criminal or civil liability or data that require stronger security measures per regulation.

- **DSL5 - Sensitive Data**: Data that could place the subject at severe risk of harm or data with contractual requirements for exceptional security measures.
What if my data is not human subjects research, Sensitive or DSL 3-5?

- Non-Sensitive, DSL 1-2 data still must comply with the HRDSP & Enterprise Security Policy requirements, for example:
  - DSL 2 likely cannot be stored or collected on (non-Harvard) commercial products
  - May require a DUA if data is being requested from, or sent to, a third party
  - **Data Ownership Policy & Legal Agreements Signature Authority** are always in play: The University is charged with protecting researchers’ rights and access to research data, which may require a DUA or other type of research agreement when data is being exchanged
Quick Takeaways!

- Non-human subjects data is still governed by the HRDSP and Enterprise Security Policy.
- The managing or supervising faculty member is responsible for ensuring that all data is handled consistent with institutional policies.
- DSL 3-5 must be submitted in the Safety Application for Security Review.
Security Review in the Safety Application
What is a Security Review?

Information Security Reviewer (ISR) will review project’s basic information design and data flow, along with:

- Planned data collection, storage, handling, transfer, archiving, sharing, and secure destruction methods
- Access controls, subject privacy practices
- The purpose of the Review is to ensure that anticipated methods meet both HRDSP and Enterprise Policy requirements, in addition to any contractually obligated requirements
- Security is here to help! If a plan does not meet policy, your ISR will provide guidance, and can facilitate connections to IT support, negotiating offices, and alternative resources as needed.
Researchers submit info related to their research data in the Safety Application for review by an Information Security Reviewer (ISR)

- Each submission creates a new draft Data Security Plan. Upon approval, receive a Security Approval Letter, with approved Security Plan
- The online forms tell you where to include info and attach any supporting documentation (DUA, data management plan, list of datapoints, vendor contract, etc.)
- Forms may contain both optional and required information, identified by a red asterisk (*)
- The Plan can cover one or more related datasets
- Plans can be updated easily, and must be confirmed annually to ensure accuracy
Quick Takeaways!

- ISR is looking for a comprehensive picture of your data’s lifecycle
- The Safety Application will suggest pre-approved resources, and notify local provisioners
- Data Security Plans must be reviewed and confirmed annually, to ensure information is accurate
  - Note: Annual training is also a requirement under the HRDSP.
DUA Review in the Agreements Application
What is a Data Use Agreement (DUA)?

- When data is confidential, proprietary, or otherwise considered restricted, the data provider (which can be Harvard) will often require a written contract to outline the terms and conditions of the data transfer.
- These agreements won’t always be called a DUA, might be Confidentiality, or Transfer Agreement/Contract (or many other names!).
- DUAs, whether incoming or outgoing, must be submitted for review in the Agreements Application by the cognizant negotiating office.
- All projects involving a DUA also require Security Review in the Safety Application, due to the additional responsibility, liability and security controls.
DUA Review Details

- The negotiating office will work with the data provider/recipient to ensure the DUA includes compliant language, and can put together a template if one isn’t provider (or the data is outgoing).

- In addition to Security Review, IRB review may also be required if the DUA involves the exchange of human subjects research data.
  - The negotiator cannot sign the DUA until both these reviews have been completed, so make sure you submit any necessary requests and Manage Related Projects as soon as you have the relevant information.
Quick Takeaways!

- DUAs **can only be signed** by a negotiating office, and therefore must go through the Agreements Application.
- All studies involving DUAs must also obtain Security Review to ensure we can comply with any security requirements, and that we’re properly managing access to the data.
- If you’re unsure as to whether a DUA is required, better safe than sorry – ask your local negotiating office!
Other types of agreements

Sponsored and vendor/consulting
If Harvard is the prime recipient of a sponsored award, the project’s data lifecycle, including use by collaborators, may need to be approved by an Information Security Reviewer in the Safety Application:

- If the sponsor imposes explicit data security terms, Security Review must be finalized prior to execution of the award (at latest)
- If the project involves Sensitive/DSL3-5 data, or data that is otherwise required by University policy to receive approval from an ISR, Security Review must be finalized prior to data collection, development or exchange.

The PI must provide the negotiating office with a copy of the Security Approval Letter (generated by Safety App) which includes any specific HU policy reqs.
Data collected, developed, or exchanged pursuant to a sponsored project

Subawards: If Sensitive/DSL3-5 data, or data that is otherwise required by University policy to receive approval from an ISR, is being exchanged with a subrecipient, Security Review must be finalized before execution of the subaward.

- Specific security requirements with respect to the subrecipient’s receipt or collection of data may be incorporated into the subaward, as applicable.
Vendor/consulting agreements must be executed with all vendors and other third parties who collect, process, host or store DSL3 or 4 information, or have access to Harvard sensitive systems.

- If the vendor will be accessing DSL4 data, they must undergo a Vendor Risk Assessment by HUIT Information Security
- Harvard’s Procurement Offices (and OGC) has created templates including approved language, and riders for PII, GDPR and other sensitive data
Quick Takeaways!

- Sensitive, DSL 3-5, regulated and proprietary data require Security Review as part of the sponsored process.

- The PI is responsible for providing the negotiating office with a copy of the applicable Security Approval Letter (covering the relevant data) for their records.

- If your data is Sensitive or DSL 3-5, and you need to hire a vendor/consultant, you should use the pre-approved templates and also may be required to obtain Security Review.
Questions?

Email rachel_talentino@Harvard.edu, or reach out to your local Information Security Reviewer, IRB or negotiating office.