HARVARD CATALYST

Harvard Clinical & Translational Science Center

VISP – Vendor Information Security Plan:

A tool for IT and Institutions to evaluate third party vendor capacity and technology to protect research data

Harvard Catalyst Regulatory Foundations, Ethics, and Law Program

Table of Contents

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Executive Summary

The Vendor Information Security Plan (VISP) is a template planning tool that enables institutions to evaluate the capacity of third party vendors to protect personally identifiable research data or other confidential information on behalf of an institution or its researchers.

The VISP may be used alone or in conjunction with the Harvard Catalyst Vendor Assessment Worksheet.[1] Use the VISP when your institution or researchers intend to utilize a vendor or third party providing software, service or infrastructure that will hold, analyze, or otherwise persistently process research data.

Institutions may present the VISP to prospective vendors for completion. Once completed, the vendor or third party returns the VISP to the institution. It is then the responsibility of the institution to undertake a review of the completed response and manage any further clarifications or negotiation of gaps in understanding of implementation requirements.

The VISP is a model template developed at Partners HealthCare in collaboration with contributions from Boston Children's Hospital, Beth Israel Deaconess Medical Center, Hebrew SeniorLife, and the Harvard Catalyst Data Protection Committee.

[1] https://catalyst.harvard.edu/pdf/regulatory/Vendor%20Assessment%20Worksheet.pdf

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Purpose and Instructions

Vendors or other third parties contemplating processing, storing, or accessing research data on behalf of an institution or its researchers should complete the following template.

Once completed, the ISP will facilitate an institution's review of vendor organizations' data safeguards and security posture including how the organization secures:

- The information technology resources used in the processing, transport, and storage of data; and
- User access to information technology resources and data.

Each template must be customized to specifically address the vendor's information technology resources and overall security posture.

Vendor Information Security Plan (VISP) Template

Vendor	
Version	
Date	

Please answer each section of the document, and attach supplemental diagrams, and any relevant policies, standards, and procedures, as appropriate. Answer the questions as specifically as possible, indicating controls actually used to safeguard information systems, applications, and data related to institution and its affiliated entities.

Institutional Oversight Contact Information

[INSTITUTIONAL CONTACT EMAIL AND ADDRESS HERE]

If you have questions, please send an email to the address above, and we will contact you.

Vendor Organizational Information Security Responsibilities

Primary Information Security Contact	
Name:	
Title:	
Organization:	
Address:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact: (name, phone & email)	

Information Security Organization, and Roles and Responsibilities

<Provide an overview of the individuals and any sub-units with security-related responsibilities.>

Systems Overview

Note: This section must be completed in its entirety. Supplemental documentation, such as SOC2 and SSAE 16 reports, are not substitutes for completing the section below. However, we welcome additional information such as the SOC, ISO and SSAE16 reports in support of your documented information security posture.

<Describe at a high-level the information technology resources used for providing applications, services and data specific to [INSTITUTION] *and its affiliates, or for accessing* [INSTITUTION'S] *-provided resources or systems. As an example, describe the software, computing environment, and data processing facilities used to host a system used by* [INSTITUTION]*, or by the vendor and its agents. Alternatively, please describe how the vendor and its agents will access resources hosted by* [INSTITUTION]*. Attach any relevant network diagrams illustrative of any system interconnections necessary for providing the solution. In this section be sure to document all methods by which data and documentation will be electronically accessed, or transmitted* [INSTITUTION]*.>*

Subcontractors

<Please indicate whether subcontractors will be used to provide any additional services under the contract with [INSTITUTION] *or its affiliates. If so, please name the subcontractors, and indicate whether the subcontractor's primary place of business or any agents perform services in locations outside the continental United States. Please indicate if the vendor has signed business associate contracts with subcontractors as required under HIPAA's Omnibus Rule.>*

Information Security Controls

When answering this section please erase the descriptive text below each header. If a particular section is not applicable to your relationship with [INSTITUTION], please indicate "not applicable", including the reasons why.

a. Access Control

<Describe the technical, operational, and management controls used to provision access to systems and data. Include how user accounts and access to data is managed for an employee over time.>

b. Awareness and Training

<Describe organizational requirements related to workforce information security awareness and training, including how employees are trained on securing devices, accounts, applications, services and data.>

c. Audit and Accountability

<Describe organizational requirements related to audit information, including what events are audited, the retention of audit information, and monitoring for unauthorized information disclosure.>

d. Certification, Accreditation and Security Assessments

<Describe how the organization certifies the information systems used for the solution are secure. Also, describe how the organization certifies the computing environments of subcontractors.>

e. Configuration Management

<Describe the organization's configuration management practices for all systems, including whether baseline configuration information is recorded, and the access restrictions implemented to enforce change management.>

f. Contingency Planning

<Describe the organization's contingency planning practices, focusing on the contingency planning practices that will affect all services provided to [INSTITUTION]*.>*

g. Identification and Authentication

<Describe the organization's identity and authentication policy, standards and procedures, including how users access [INSTITUTION] services*, Systems, data and how those users are identified and authenticated.>*

h. Incident Response

<Describe the organizations incident response capabilities, including incident response, monitoring and reporting capabilities.>

i. Maintenance

<Describe the organization's system maintenance policy and procedures, including requirements related to any remote system maintenance performed by third parties.>

j. Media Protection

<Describe organizational requirements for securing storage media, including back-up tapes, failed hard drives, and other storage media.>

k. Physical and Environmental Protection

<Describe organizational requirements for securing data processing facilities, including data centers, and the computing environments of individuals.>

l. Planning

<Describe how information security planning activity is incorporated into overall business planning, including whether system security plans are documented for systems and services.>

m. Personnel Security

<Describe the organization's personnel security controls, including employee screening, access agreements, and termination procedures.>

n. Risk Assessments

<Describe the organization's approach for assessing risk, including whether formal risk analysis are performed, and whether vulnerability assessments are performed for the information technology resources used for the solution.>

o. System and Services Acquisition

<Describe how information security is part of the organization's acquisition of information systems and services.>

p. System and Communications Protection

<Describe the organization¹s communication security policies, standards and procedures, including the organization¹s secure transmission capabilities, and how the organization secures the information technology resources from external threats. This section should also describe the controls implemented to secure data and documentation as it is transmitted over untrusted networks (e.g., the internet).>

q. System and Information Integrity

<Describe how the systems ensure the integrity of data, including malicious code protection, input validation, and other related techniques. >

Terms of Use

We encourage broad dissemination of this guidance document, and incorporation of these practices into clinical trial operations. We would also appreciate feedback and additional contributions so that we can continuously improve this work product.

We encourage you to:

- **request** — email us and request the materials
- **share** — copy, distribute, and transmit the work
- **adapt** — adapt the work to suit your needs

Under the following conditions:

- **Attribution**: We encourage the broad dissemination of this tool. In freely using the materials, we require that you acknowledge Harvard Catalyst as the publisher and that you give appropriate credit to any named individual authors.

- **Suggested citation:** *This material is the work the Harvard Catalyst Data Protection Taskforce and subcommittee of the Regulatory Foundations, Ethics, and Law Program. This work was conducted with support from Harvard Catalyst | The Harvard Clinical and Translational Science Center (National Center for Research Resources and the National Center for Advancing Translational Sciences, National Institutes of Health Award 1UL1 TR001102-01 and financial contributions from Harvard University and its affiliated academic health care centers). The content is solely the responsibility of the authors and does not necessarily represent the official views of Harvard Catalyst, Harvard University and its affiliated academic health care centers, or the National Institutes of Health.*

With the understanding that:

- **We might contact you**: We are interested in gathering information regarding who is using the material and how they are using it. We may contact you by email to solicit information on how you have used the materials or to request collaboration or input on future activities.
- **When reusing or distributing, make clear the above terms**: For any reuse or distribution, you must make clear to others the terms of this work. The best way to do this is with a link to the web page containing this guide.
- **When adapting**: Please share improvements to the tool back with us so that we may learn and improve our materials as well.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Contact Us

We welcome any feedback or questions you may have. Please email us at regulatory@catalyst.harvard.edu.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).