THE HARVARD CLINICAL
AND TRANSLATIONAL
SCIENCE CENTER

Vendor Assessment Worksheet:

A sample set of IT security controls for evaluation of third party vendors' capacity to protect institutional research data

Table of Contents

Executive Summary

This worksheet may be used alone or in conjunction with the *Harvard Catalyst Vendor Information Security Plan*.

This worksheet offers a list of data security controls that institutions may require that vendors or other third parties implement to protect "confidential data."

As used here, "confidential data" refers broadly to any data that an institution considers to merit a heightened degree of protection because unauthorized release of the information may present a risk of physical, psychological, or financial harm to an individual.

This worksheet was adapted from a Harvard University template for evaluation of systems, servers, technology, and/or platforms holding data classified at a risk of level 3 on a 5 level scale, 5 representing the highest degree of risk.

Use this worksheet 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 Vendor Assessment to prospective vendors for completion. Once completed, the vendor or third party returns the Assessment to the institution. It is then be the responsibility of the institution to undertake a review the completed response and manage any further clarifications or negotiation of gaps in understanding of implementation requirements.

Institutions are encouraged to establish both baseline research data security standards along with sets of standards and controls adaptable on a project-by-project basis, which adhere to risk based frameworks.

Sample Security Control Requirement	Met (Y/N)	How Met
1. Network Security Requirements		
1.1. [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] must not be directly accessible from the Internet or from open parts of the [INSTITUTIONAL] networks unless the confidential information is encrypted. (Note that use of a VPN concentrator is not considered "direct access.")		
1.2. Servers holding [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] connected to any network must run host-based firewalls configured to block all connections to the system other than the specific types of connections needed to perform the approved functions.		
1.3. Documented practices must be in place and followed on maintaining the configurations of the host-based firewalls.		
1.4. The [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] must be encrypted when it traverses any network (outside of a switch in a secure information center).		
1.5. The [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] must never be sent via email except in encrypted files.		
1.6. All users needing to transfer the [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] must make use of a secure transfer method. (e.g., Accellion or encrypted email).		

Sample Security Control Requirement	Met (Y/N)	How Met
2. System security requirements:		
2.1. Administrative functions on the SECURE SERVERS or applications that access the information must be logged. The logs should include the identity of the user, the time, and the command executed.		
2.2. Generic accounts on systems must be disabled.		
2.3. Default passwords on systems must be changed before systems are put into use.		
2.4. A mechanism must be in use on SERVERS HOLDING ["CONFIDENTIAL INFORMATION" OR ALTERNATIVE DATA CLASSIFICATION TERM] to inhibit attackers guessing passwords (e.g., lockout after multiple bad password guesses).		
2.5. A mechanism must be in use on servers or clients to block access to idle sessions (e.g., an application timeout or a locking screen saver).		

Sample Security Control Requirement	Met (Y/N)	How Met
3. Operational requirements:		
3.1. All media (including magnetic media such as portable disk or thumb drives and non-magnetic media such as optical disks or paper) containing the confidential information must be encrypted or secured in a locked container (e.g., a file cabinet or safe) when not actually in use.		
3.2. Where access to systems storing the information from outside of the premises is permitted, there must be a written policy identifying individuals or categories of persons who have permission, and under what conditions ("The remote access policy").		
3.3. Users must only have access to the [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] through their individually assigned (non-shared) user accounts.		
3.4. Users' access to [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] or servers must be removed if they no longer have a reason under the access policy to access the information (e.g., they change jobs or leave the institution).		
3.5. [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] servers must enforce standard password complexity rules.		
3.6. SERVERS HOLDING [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] and the applications that process the confidential information must be designed so that passwords cannot be retrieved by anyone (including system administrators). (This should include a mechanism to ensure that any assigned passwords are changed on initial use.)		
3.7. Interactive access to SERVERS HOLDING [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] must be logged. The logs should include the identity of the user, the time, and the function (login or logout).		
3.8. The logs should be reviewed periodically to determine if the systems are under attack and that the users are following the documented access practices (e.g., not logging in as root).		

Sample Security Control Requirement	Met (Y/N)	How Met
3.9. There must be a documented practice, known by the users, to ensure that any possible breach that might put the confidential information at risk is promptly reported to the [APPROPRIATE INSTITUTIONAL OFFICE].		
3.10. The confidential information is not permitted to be stored on any user computer or portable computing device (e.g., laptop, PDA, or smart phone) unless the information is encrypted.		
3.11. The appropriate [INSTITUTIONAL OFFICES] must be informed of any plans to have a vendor store or process the confidential information.		
3.12. Contracts must be executed with all external vendors who process or store the [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] at INSTITUTION'S direction.		
3.13. The contracts must contain specific contract language (approved by INSTITUTIONAL OFFICE) that requires the vendor to protect the [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] and to inform [APPROPRIATE INSTITUTIONAL OFFICE] of any possible breach that may put the information at risk of exposure.		
3.14. The contracts must contain specific contract language [APPROVED BY APPROPRIATE INSTITUTIONAL OFFICE] to ensure that the protection of the confidential information meets the requirements in INSTITUTION'S information security policy.		
3.15. Controls must meet conditions of institutional contract rider specifications		
3.16. All software (operating system and application) patches must be up to date.		
3.17. Only the applications that are actually required to support the required services can be running on a SECURE SERVER.		
3.18. [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] must be running an appropriate virus checker and the virus checker information files must be updated at least weekly.		

Sample Security Control Requirement	Met (Y/N)	How Met
3.19. Operators of non-IT-managed servers holding ["CONFIDENTIAL INFORMATION" OR ALTERNATIVE DATA CLASSIFICATION TERM] must annually certify to [INSTITUTIONAL OFFICE] that they are compliant with the [INSTITUTIONAL POLICY].		
3.20. [INSTITUTIONAL] employees working with any kind of ["CONFIDENTIAL INFORMATION" OR ALTERNATIVE DATA CLASSIFICATION TERM] should undergo training in general information security at least annually.		
3.21. [INSTITUTION] owned systems should be scanned at least annually to ensure that designated information is stored on the system.		
3.22. Implementation of operational requirements is subject to review and audit by [INSTITUTIONAL OFFICES]		

Sample Security Control Requirement	Met (Y/N)	How Met
4. Information Collection		
4.1. Collection of [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] while in the field must adhere to [INSTITUTIONAL POLICY].		
4.2. Computer-based collection of [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] in the field may be done using a VPN connection to a secure server.		
4.3 Computer-based collection of [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] information in the field may be done using a computer with an encrypted disk. Information collected in the field must be transferred (by secure means) to systems incorporating appropriate SAFEGUARDS at the earliest possible opportunity, and then promptly and securely deleted from the field device (laptop, digital recorder, etc.).		

Sample Security Control Requirement	Met (Y/N)	How Met
5.0 Managing Pre-Existing Databases		
5.1 Collection of [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] while in the field must adhere to [INSTITUTIONAL POLICY].		
5.2. Computer-based collection of [“CONFIDENTIAL INFORMATION” OR ALTERNATIVE DATA CLASSIFICATION TERM] FROM A PRE-EXISTING DATABASE may be done using a VPN connection to a secure server.		

CORE WRITING GROUP

Last Name	First Name	Company/ Affiliation
Zurba	Joe	Partners HealthCare
Bolt	Kris	Harvard University
Edmiston	Scott	Harvard Catalyst
Winkler	Sabune	Harvard Catalyst

CONTRIBUTORS

Recognizing those that contributed specific content, templates or examples that are included within this guidance document:

Last Name	First Name	Company/ Affiliation
Aske	Jennings	Partners HealthCare (formerly)
Kane	Esmond	Harvard University (formerly)
Steve	Berry	Beth Israel Deaconess Medical Center
Jason	Rightmyer	Hebrew Senior Life
David	St. Clair	Boston Children's Hospital

ATTRIBUTION, SHARING AND ADAPTING

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**: 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.

CONTACT US

Copies of all materials are freely available. Please send your requests, questions and comments to *regulatory@catalyst.harvard.edu* and visit the Harvard Catalyst Data Protection Subcommittee web page.