IT Security Best Practices

For NIH HIV/AIDS Clinical Trials Network Sites and Labs

Version 5.0 | January 2022

Table of Contents

1.0 Introduction

This document was prepared by the Information Technology Best Practices Working Group (ITBPWG) facilitated by the Office of HIV/AIDS Network Coordination (HANC). It is intended for clinical research sites and laboratories affiliated with the U.S. National Institutes of Health (NIH) HIV/AIDS Clinical Trials Networks.

The best practices contained in this document should be viewed as recommendations only, and are not enforced through the NIH Division of AIDS (DAIDS) clinical site and study monitoring.

1.1 The IT Best Practices Working Group

The IT Best Practices Working Group (ITBPWG) is facilitated by the Office of HIV/AIDS Network Coordination (HANC) to serve as an oversight body for technological standards across clinical research sites and laboratories affiliated with the NIH HIV/AIDS Clinical Trials Networks. The group convenes on a

biennial basis to review information technology and security best practices and publish guidance to support site and lab alignment to modern IT guidelines.

The ITBPWG includes representatives from the DAIDS, the NIH Office of Cyber Infrastructure and Computational Biology (OCICB), SCHARP, Frontier Science, and HANC.

1.2 Background

Over the years, several notable changes have shifted the ITBPWG's approach to site information technology and data security. First, many research sites now use electronic data capture systems, web-hosted software, and cloud infrastructure in place of locally-installed software to support clinical trials data collection and management. This movement away from on-premise installations has reduced cost, set-up, and maintenance obligations for sites and their local IT environment; and redefined security responsibilities for sites as end-users, software hosts, and software-as-a-service (SaaS) / cloud providers.

Second, the COVID-19 pandemic has and continues to cause major disruption to clinical trial conduct. Notably, it has catalyzed the adoption of hybrid or fully decentralized clinical trials (DCTs) and of digital health technologies to support clinical research (1). This increase in digital innovation and use of tools such as electronic consent (eConsent), telehealthcare, electronic clinical outcome assessments (eCOA), and electronic patient reported outcomes (ePRO) broadens the possibilities for more effective clinical trial management, data collection, and trial participant engagement. However, they likewise introduce additional cybersecurity risks to clinical trials that can impact multiple parties across the research enterprise, including the trial sponsor, clinical research organizations (CROs), research sites and their affiliated institutions, investigators, and trial participants. Countries and/or expert committees may have also issued guidance specific to COVID-19 and its impact on clinical trials conduct and participants with HIV (2-4). If existing, these too should be consulted in the development of mitigation plans.

Lack of adequate standards and safeguards in information technology practice can disrupt essential clinical site operations, hamper research, and compromise study results. Observing established information security standards can mitigate these disruptions while safeguarding participant privacy and study integrity. Sites should ensure appropriate plans are in place to protect their local IT network security, to protect all systems used at the site during the conduct of a clinical trial, and to mitigate risks resulting from disruptions or delays to study activities (5). To this end, the *IT Security Best Practices: Cybersecurity Framework* outlines a recommended approach for research sites and labs participating in the NIH-funded HIV/AIDS Clinical Trials Networks to manage information technology and cybersecurity risks.

1.2 How to Use the Cybersecurity Framework

The ***Cybersecurity Framework***, hereafter referred to as the *Framework*, is designed to complement existing site and/or institutional processes for privacy and cybersecurity risk management. It is not designed to replace existing processes. Rather, an organization should overlay its current processes onto

the *Framework* to assess gaps in the current cybersecurity risk approach and develop a plan for improvement. Sites or organizations that do not have an existing cybersecurity program may use the *Framework* to help establish one.

Overall, the *Framework* provides a standard process to help sites:

1. Describe their current cybersecurity posture
2. Describe their target state for cybersecurity
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. Assess progress toward the target state
5. Communicate among internal and external stakeholders about cybersecurity risk

Sites will have unique risks dependent on their local environment, vulnerabilities, threats, and risk tolerances. As a result, sites may vary in how they customize practices described in the Framework and may prioritize activities that are essential to site operations or that yield the greatest benefit per resource spent. Ultimately, the goal is to reduce and improve management of cybersecurity risks.

The Framework is organized around five basic cybersecurity **Functions** at a high level: Identify, Protect, Detect, Respond, and Recover. These *Functions* are not meant to form a sequential path or lead to a static end state. Rather, they should be performed concurrently and continuously to develop a culture that is dynamic and adaptive to IT security risks (6-7).

Related DAIDS Requirement(s) are DAIDS guidance documents and/or policies that describe sponsor requirements related to or overlapping with the Framework activity. They are primarily based on the DAIDS Site Clinical Operations and Research Essentials (SCORE) Manual (8), published DAIDS Clinical Research Policies (9), and required standard operating procedures (SOPs) for clinical research sites conducting DAIDS-sponsored studies within the DAIDS Clinical Trials Networks. The listed *Related DAIDS Requirement(s)* are illustrative and not exhaustive of all potential sponsor requirements.

2.0 Cybersecurity Framework

Adapted from: NIST Special Publication 1271, Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide (10).

2.1 Identify

Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Activity	Description	Related DAIDS Requirement(s)
Identify critical site processes and assets	What are your site's activities that absolutely must continue in order to be viable? For example, this could be submitting clinical data, managing randomization systems, documenting electronic informed consent from study participants, or ensuring that the information your site collects remains accessible and accurate.	DAIDS SCORE Manual, Introduction to DAIDS Systems List of SOPs Required at Clinical Research Sites
Maintain hardware and software inventory	It's important to have an understanding of the computers and software at your site because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet.	The DAIDS EIS Policy Appendix A (Section 7.0) states that SOPs should be established for *Change Control*.
Document information flows	It's important to not only understand what type of information your site collects and uses, but also to understand where the data is located and how it is used, especially where contracts and external partners are engaged.	
Establish policies for cybersecurity that	These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical site	The DAIDS EIS Policy Appendix A (Section 7.0) states that SOPs should be established for *Access and*

include roles and responsibilities	processes. Cybersecurity policies should be integrated with other site risk considerations (e.g., financial, reputational).	*Authentication*, *Data Collection and Handling*, *Security*, and *Information Security*.
Identify threats, vulnerabilities, and risk to assets	Sites should ensure risk management processes are established and managed to ensure that internal and external threats are identified, assessed, and documented in a risk assessment. Ensure risk responses are identified and prioritized, executed, and results monitored.	

2.2 Protect

Develop and implement the appropriate safeguards to ensure delivery of services.

Activity	Description	Related DAIDS Requirement(s)
Manage access to assets and information	Create unique accounts for each person working with data and ensure that users only have access to information, computers, and applications that are needed for their jobs. Do not share accounts between users. Authenticate users with multi-factor techniques before they are granted access to information, computers, and applications (password-only solutions are not compliant with NIH standards). Tightly manage and track physical access to devices.	DAIDS EIS Policy DAIDS EIS Policy Appendix A (Sections 1.0, 7.0) DAIDS EIS Policy Appendix B (Sections 2.0, 4.0, 7.0) The List of SOPs Required at Clinical Research Sites includes *Access and Authentication*

Protect sensitive data	If your site stores or transmits sensitive data, make sure that this data is protected by encryption both while it's stored on computers as well as when it's transmitted to other parties. Consider utilizing integrity checking to ensure only approved changes to the data have been made. Securely delete and/or destroy data when it's no longer needed or required for compliance purposes.	DAIDS EIS Policy Appendix A (Sections 5.0, 9.0) DAIDS EIS Policy Appendix B (Sections 5.0, 12.0) DAIDS SCORE Manual, Essential Documents The List of SOPs Required at Clinical Research Sites includes *Data Collection and Handling*, *Data Integrity*, and *Retention of Study Records Including Electronic Records - Long Term Storage*.
Conduct regular backups	Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware and perform routine tests to verify the integrity of the backup.	DAIDS EIS Policy Appendix A (Section 4.0) The DAIDS EIS Policy Appendix A (Section 7.0) states that SOPs should be established for *Data Backup, Recovery, and Contingency Plans*. DAIDS EIS Policy Appendix B (Section 3.0)
Protect your devices	Consider installing host based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and that devices are disposed of securely.	The DAIDS EIS Policy Appendix A (Section 7.0) states that SOPs should be established for *Security* and *Information Security.*

Manage device vulnerabilities	Regularly update both the operating system and applications that are installed on your computers and other devices to protect them from attack. If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.	DAIDS EIS Policy Appendix A (Sections 1.1, 5.0) The DAIDS EIS Policy Appendix A (Section 7.0) states that SOPs should be established for *System Maintenance.* DAIDS EIS Policy Appendix B (Sections 8.0)
Train users	Regularly train and retrain all users to be sure that they are aware of site cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment.	DAIDS EIS Policy DAIDS EIS Policy Appendix A (Section 6.0) DAIDS EIS Policy Appendix B (Sections 9.0) The List of SOPs Required at Clinical Research Sites includes *Personnel Qualifications* and *Personnel Training and Certification Documentation.*

2.3 Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Activity	Description	Related DAIDS Requirement(s)

Test and update detection processes	Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting both within your site, institution, and to external governance and legal authorities.	
Know the expected data flows for your site	If you know what and how data is expected to be used for your site, you are much more likely to notice when the unexpected happens – and unexpected is never a good thing when it comes to cybersecurity. Unexpected data flows might include clinical information being exported from an internal database and exiting the network. Your site or institution may have contracted work to a cloud or managed service provider; discuss with them how they track data flows and report, including unexpected events.	
Maintain and monitor logs	Logs are crucial in order to identify anomalies in your site's computers and applications. These logs record events such as changes to systems or accounts as well as the initiation of communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.	
Understand the impact of cybersecurity events	If a cybersecurity event is detected, your organization should work quickly and thoroughly to understand the breadth and depth of the impact. Seek help. Communicating information on the event with appropriate stakeholders will help keep you in good stead in terms of partners, oversight bodies, and others and improve policies and processes.	

2.4 Respond

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Activity	Description	Related DAIDS Requirement(s)
Ensure response plans are tested	It's even more important to test response plans to make sure each person knows their responsibilities in executing the plan. The better prepared your site is, the more effective the response is likely to be. This includes knowing any legal reporting requirements or required information sharing.	
Ensure response plans are updated	Testing the plan (and execution during an incident) inevitably will reveal needed improvements. Be sure to update response plans with lessons learned.	
Coordinate with internal and external stakeholders	It's important to make sure that your site's response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.	

2.5 Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event (8).

Activity	Description	Related DAIDS Requirement(s)

Communicate with internal and external stakeholders	Part of recovery depends upon effective communication. Your recovery plans need to carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need but no inappropriate information is shared.	
Ensure recovery plans are updated	As with response plans, testing execution will improve employee and partner awareness and highlight areas for improvement. Be sure to update Recovery plans with lessons learned.	
Manage public relations and institution/CRS reputation	One of the key aspects of recovery is managing the site's reputation and relationship with study participants. When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – and not reactionary.	

3.0 References

1. De Brouwer W, Patel CJ, Manrai AK, Rodriguez-Chavez IR, Shah NR. Empowering clinical research in a decentralized world. Npj Digit Med. 2021 July 1;4(102). Available from: https://doi.org/10.1038/s41746-021-00473-w
2. U.S. Food and Drug Administration (FDA). FDA guidance on conduct of clinical trials of medical products during the COVID-19 public health emergency. 2021 Aug 30. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/fda-guidance-conduct-clinical-trials-medical-products-during-covid-19-public-health-emergency
3. South African Health Products Regulatory Authority (SAHPRA). SAHPRA policy on conduct of clinical trials of health products during the current COVID-19 pandemic. 2020 Mar 25. Available from: http://www.sahpra.org.za/wp-content/uploads/2020/03/SAHPRA-Communication_COVID_19-Final-25032020.pdf
4. European Medicines Agency (EMA). Guidance on the management of clinical trials during the COVID-19 (coronavirus) pandemic, Version 4. 2021 Apr 2. Available from: https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-10/guidanceclinicaltrials_covid19_en.pdf
5. Bacchieri A, Rossi A, Morelli P. Risk and mitigation actions for clinical trials during COVID-19 pandemic (RiMiCO). Contemp Clin Trials Commun. 2020 Dec;20(100682). Available from: https://doi.org/10.1016/j.conctc.2020.100682
6. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2018 Apr 16. Available from: https://doi.org/10.6028/NIST.CSWP.04162018
7. National Institute of Standards and Technology [Internet]. Cybersecurity Framework. [cited 2021 Dec 20]. Available from: https://www.nist.gov/cyberframework
8. Division of AIDS [Internet]. DAIDS Site Clinical Operations and Research Essentials (SCORE) Manual. 2021 Nov 3 [cited 2021 Dec 20]. Available from: https://www.niaid.nih.gov/research/daids-score-manual Mahn A, Marron J, Quinn S,
9. Division of AIDS [Internet]. DAIDS Electronic Information Systems (EIS) Policy. 2021 Aug 24 [cited 2021 Dec 20]. Available from: https://www.niaid.nih.gov/research/daids-clinical-site-implementation-operations
10. Topper D. Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. 2021 Aug. Available from: https://doi.org/10.6028/NIST.SP.1271

4.0 About

4.1 The NIST Cybersecurity Framework

The ITBPWG's *Cybersecurity Framework* is based on the U.S. National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (6). Version 1.0 of the NIST Cybersecurity Framework was published in 2014 and updated to Version 1.1 in 2018. The NIST Cybersecurity Framework is built from effective practices to help organizations improve their cybersecurity program. It presents a consistent approach to identifying, assessing, and managing cybersecurity risk to critical infrastructure.

5.0 Revision History

Version No.	Release Date	Notes
v1.0	Feb 22, 2012	Initial release
v2.0	Jan 23, 2013	
v3.0	Mar 10, 2016	
v4.0	Dec 18, 2018	Updates to minimum and ideal IT standards
v5.0	Jan 12, 2022	Significant revisions based on NIST cybersecurity framework.