Information Technology Best Practice Standards at NIH HIV/AIDS Clinical Research Networks' Study Sites and Site Affiliated Laboratories

Document collaborators: Frontier Science & Technology Research Foundation (FSTRF), Office of HIV/AIDS Network Coordination (HANC), Office for Cyber Infrastructure & Computational Biology (OCICB), Office of Clinical Site Oversight (OCSO), and the Statistical Center for HIV/AIDS Research & Prevention (SCHARP)

Background and Rationale

The National Institutes of Health's (NIH) Division of AIDS (DAIDS) has been conducting clinical and observational HIV/AIDS clinical trials for over thirty years. This work and the technological development of affiliated sites and laboratories have grown organically: international sites[1] have increased in number and extended their working relationships to multiple DAIDS networks. For sites receiving funding from multiple sources, it is very common to share their infrastructure, including data-acquisition devices, for different studies across different networks.

The very nature of HIV/AIDS research requires laboratory and clinical operations in resource-limited regions. While they might establish a technical infrastructure that is adequate for accomplishing the broad task, they are not following international standards (e.g., ISO 27017/27018/27001) or are without the financial or personnel resources to establish a solid IT infrastructure or maintain IT and data management best practices. This can hold true for sites in and outside of the United States. Through the act of running technical equipment at sites for the purpose of data collection and transfer, the Statistical and Data Management Centers (SDMCs) become as much a user of the site infrastructure as the site staff. If there is a power outage, a downed internet connection, or a failed hard disk, the SDMCs often assume responsibility for troubleshooting and resolving problems.

Different organizations—between and across networks—may have different technical needs and requirements for each other, and these requirements may be subtle. Without standards and collective oversight, changes made at one site can affect the work of another by "breaking" essential systems. This in turn can hamper research and/or compromise results. These are not hypothetical dangers: over the past ten years, sites have irretrievably lost data from crashed hard disks and viruses. Conforming to an established technical infrastructure standard can mitigate these losses.

Due to the role played by the SDMCs as the data receivers, managers, and analyzers, SDMCs have a partnership with the sites and a vested interest in their success. As such, the SDMCs are users of the sites' technical infrastructure, which can be regarded as equipment vital to study operations. Not all technological devices can work with each other flawlessly. In many cases, these exceptions are difficult to capture in a standard. For example:

- The SDMCs often use specific solutions for transferring data or providing remote assistance to a site. They can require specific "ports" to be accessible from the internet to the site or vice versa. A change by the site's internet service provider or the site IT management team aimed at improving security or performance can block access to these ports and the site will find that they are unable to upload the data to the SDMC. Therefore, implementation of these technologies (including - Packet Shaping, Quality of Service) should be coordinated with the SDMCs to avoid side effects.

As more networks and sites come online, the potential for conflict increases proportionally. Conflicts can be mitigated with technological standards, an oversight body to ensure conformance, and increased communication among the DAIDS stakeholders in the sites' technical infrastructure.

[1] Unless otherwise mentioned, the term 'site' is used inclusively for both the clinical site and site-affiliated laboratories.

Process

1. Representatives from DAIDS, the SDMCs, site technical stakeholders, and any other critical partners will constitute the IT Best Practices Task Force (ITBPTF).
2. The ITBPTF serves as the oversight body, responsible for establishing a set of baseline technological standards for sites and laboratories, both domestic and international. This body will convene biennially on even years to revise and update the "Information Technology Best Practice Standards at NIH HIV/AIDS Clinical Research Networks' Study Sites and Site Affiliated Laboratories" document to be in accordance with modern guidelines.
3. This oversight body will maintain a coordinated channel of communication to share technological issues and information relevant across networks and knowledge areas and discuss training and technological milestones (e.g., switching over to a new internet connection).
4. Note that OCSO clinical site and study monitoring does not include monitoring for compliance to the standards in this document.

Baseline Technological Standards

A baseline technological standard needs to consider the diversity of international locations where clinical trials might take place and respect the fact that basic work can still be accomplished in resource-limited environments at a reasonable level of cost (this cost includes both monetary and personnel).

This baseline technological standard represents two levels: "minimum" and "ideal". Sites/labs with different degrees of resources and infrastructure should scale their facilities to an appropriate standard, barring circumstances where it is logistically impossible to attain that standard. Likewise, laboratories and repositories have a different set of technical requirements that are not discussed here, such as backup power supplies for freezers.

The proposed baseline technological standards and practices are divided into the following nine categories:

1) Power Stability/Reliability

a) Minimum

i) For sites/labs where power outages occur more than twice annually, all workstations, servers and other mains-powered (i.e., AC-powered) computing equipment (such as data-acquisition devices) must be on an uninterruptible power supply (UPS), such as a stand-alone battery-based unit, or an inverter/rectifier/battery solution. The battery solution should be tested on a regular basis to ensure it is working properly. Batteries in these systems need to be replaced biannually.

ii) 220-240v Line-line-interactive UPSs.

iii) Verify and implement grounding if not already implemented (use grounding testers for verification). Do not use adapters to bypass grounding.

iv) Several type E/F and G plug adapters.

v) Automatic Voltage Switches are an inexpensive solution to protect equipment against unstable current.

b) Ideal

i) Power reliability needs to be at 99.9%+ uptime.

ii) A site/lab backup power generator with automated failover.

iii) Main power is properly conditioned to protect against current, voltage, and frequency fluctuations.

iv) There should be some system in place to monitor and provide alerts if the line current is off for long enough to require system shutdowns.

v) Automated server shutdown software under low battery conditions for graceful power down in blackouts.

vi) Network-based UPS monitoring and alerting.

vii) On-line UPSs with 24-month battery life cycle replacements.

viii) Diesel level monitored with supply chain funding and service contracts.
ix) Generator maintenance contracts in place.
x) Photovoltaics and renewable energy sources.
xi) Isolated grounding for network infrastructure.
xii) Purchase laptops in place of desktops where possible (lower draw and built-in battery).
xiii) Purchase flexible voltage equipment with 110-240 voltage ranges where possible. Avoid using step down converters.

2) Data and telecommunications

a) Internet connectivity

In general, performance and usability of systems that use the Internet to transmit data between a client and server (e.g., email, clinical data management system) increase as connection bandwidth increases and latency decreases. Conversely, performance and usability of those same systems will decrease as the number of concurrent users increase. Sites with a relatively high number of concurrent users will need to either increase connection bandwidth or reduce performance and usability expectations.

Sites can assess Internet bandwidth by referring to the following website: http://www.needhosting.net/bw/index.php.

i) Minimum

	Concurrent users		
Activity	**1-10**	**11-40**	**40+**
Email	1 Mbps	2 Mbps	5 Mbps
+ EDC	2 Mbps	4 Mbps	10 Mbps

i) Ideal

A connection with 10 Mbps of bandwidth and very low latency.

b) Phone line

i) Minimum

The site and lab are each required to have a phone line (either a land line or an institutionalized cellular phone connection) with 95% or greater uptime, and of high-enough quality to

(1) send and receive a fax, and
(2) use a 19.2k or faster modem.

3) Local-Area Network/Local Wireless Network

a) Minimum

i) The site and/or lab must maintain an Ethernet local-area network (LAN) of 100 Mb/s or greater.
ii) The LAN must be securely connected to the Internet connection with a firewall.
iii) There must be a site configurable mechanism in place to allow authorized external users limited remote access to the LAN (such as VPN).
iv) The site and/or lab should ensure that SDMC staff members have appropriate access to provide support and perform required procedures with a firewall in place.
v) Wireless networks should use WPA2-PSK or WPA2-Enterprise to protect and control access. Note: this precludes the use of 802.11b modems; 802.11g or better is needed.

b) Ideal

i) The ideal should also include network admission and quarantine control. This could be accomplished with something as simple as MAC address filtering on the site's DHCP server or wireless access points.
ii) Infrastructure Management as a Service, which can be used to easily manage networks remotely. Reference section 4(c) for provider requirements.

4) Data Backup/Recovery and Disaster Recovery Plan

a) Minimum
   i) Data backup procedures must be documented, maintained, and observed (including the daily backup of daily, incremental data).
   ii) The data-backup procedures must adhere to IT best practices (dependent on site needs—these will be variable) and include return-time objective, return-point objective, and off-site backup.
   iii) Procedures for file recovery and disaster recovery must be documented and regularly practiced, to evaluate their effectiveness.
   iv) The National Institute of Security and Technology (NIST) offers guidance on backup procedures and other security measures. Please refer to the following website for additional guidance: http://csrc.nist.gov/index.html.
   v) Centralized file and applications server: An internet-based file server system to facilitate data backup and sharing can be used. Note that because internet-based systems are not HIPAA-compliant, no participant or other sensitive information should be saved on this type of server. Reference section 4(c) for provider requirements.

b) Ideal
   i) Image-level backup, encrypted, and located off-site (physically removed from building in a secure, environmentally protected location).
   ii) Centralized file and applications server:
      (1) The site and/or lab should have a centralized file server to facilitate data backup and sharing.
      (2) An application server should be used when possible or practical to simplify the updating of software.

c) SaaS independent certifications
   i) SaaS provider needs to have a privacy statement in compliance with the General Data Protection Regulation (GDPR).
   ii) SaaS provider needs to meet ISO 27017, ISO 27018, and ISO 27001 requirements.
   iii) Data should be encrypted during transit between the localhost and backup SaaS provider.

5) Security

General security requirements apply to networked and stand-alone computers, such as Chromebooks, in addition to mobile devices used in the course of a clinical protocol (including but not limited to phones and tablets).

a) Minimum

General

   i) The site maintains a directory service for central authentication, auditing, and authorization such as Microsoft Active Directory and Azure Active Directory, Apple Open Directory, and OpenLDAP.
   ii) Users must be managed with accounts that have secure passwords with a minimum length of 12 characters. Passwords must be rotated every 180 days.
      (1) REFEDS Single-factor authentication (SFA) profile defines guidelines for single-factor authentication, such as passwords.

iii) All computers used regularly on the network must have no local administrator rights for the user accounts and autorun must be disabled.
iv) The site and lab must have adequate physical security for their facilities to ensure that access to patient files, specimens and equipment is limited to authorized personnel. Any software or devices being used for a study should maintain an audit trail, tracking who accessed it to ensure only authorized personnel have access to sensitive information.
v) The site and lab must have adequate network security to protect data and facilities from unauthorized access.
vi) The site and/or lab staff should complete security training and sign an oath of confidentiality or similar document.
    (1) NIH offers a free training found at: http://irtsectraining.nih.gov/public.aspx

Mobile and Tablet Operating Systems
vii) The site is required to have a documented mobile device management policy in place.

b) Ideal

General
i) Fulfillment of REFEDS Multi-Factor Authentication (MFA) Profile requirements.
ii) Full disk encryption of sensitive data on all desktop and mobile computers and devices that contain participant data.
iii) The Center for Internet Security (CIS) Benchmarks for IT system and data security was developed through a collaborative effort between public, private, and academic entities and subject-matter experts. Site computers should adhere to these configuration guidelines to reduce the risk of data loss or interruption to Internet access.
    (1) Configuration guidelines can be found at: https://www.cisecurity.org/cis-benchmarks/

Mobile and Tablet Operating Systems
iv) Data housed on mobile and/or tablet devices must be geotagged and encrypted.
v) Mobile and/or tablet devices must also force patching of operating system software, employ screen timeouts, enable single-application mode.
vi) Mobile devices must include a mobile device management (MDM) system that enforces remote wipe of lost or stolen systems.

c) Anti-virus/Spyware protection

Selection of antivirus tools can be difficult. In general, you may safely use antivirus/anti-spyware software built into the operating system. There are many "free" solutions available and some of them are effective. The Virus Bulleting website offers a tool for evaluating different vendors for their effectiveness (https://www.virusbtn.com).

i) Minimum
    (1) All computers/servers have the native operating system anti-virus software enabled and the latest virus definitions installed. For computers without Internet connections, a procedure for updating virus definitions must be in place.
    (2) Computers must be locked down in their configuration so that viruses cannot be accidentally installed by users.
ii) Ideal
    (1) Minimum protection level must also include removing local administrator privileges.

(2) Up-to-date best practices for anti-virus and anti-spyware prevention must be documented, maintained, and observed for each workstation, server, and laptop.
(3) A central system manages the antivirus applications on all desktops, laptops, and servers, alerting IT staff of failures in updates, virus outbreaks, etc.
(4) A central system for verifying that all computers at the site are locked down as described – for example active directory with USGCB Group Policy Objects.
(5) SaaS solutions – reference section 4(c) for provider requirements.

6) IT Training, Documentation and SOPs/WPGs

a) Minimum
   i) Site/lab IT staff need to be trained in IT best practices and "The Information Technology Best Practice Standards at Division of AIDS Clinical Trials Study Sites and Site Affiliated Laboratories" document should be made available to staff. HANC will maintain the document and keep it accessible to sites on its website. The document will be disseminated to clinical trial units and then to the clinical research sites.
   ii) Site/lab IT staff must be trained in Good Clinical Practice.
   iii) SOPs/WPGs need to be maintained, available, and complied with.
   iv) SOPs/WPGs need to have change control, and major changes should include approval from representatives from the SDMCs.

b) Ideal
   i) Monitoring and Alerting
      (1) Escalation tables
      (2) SMS alerts

7) Standard Applications and Documentation Storage Formats

a) Sites and/or labs should have the ability to create and view Microsoft Office Word, Excel, and PowerPoint and PDF files using supported versions of each product. Software used should be within two versions of the most recently released software.
b) Alternatively, use free office applications that are compatible with Microsoft Office. Examples, such as LibreOffice and Google Docs, can be found here:
   i) LibreOffice: http://www.libreoffice.org
   ii) Google Docs: https://www.google.com/docs/about/
   iii) Office 365: https://www.office.com/
c) For PDF files, sites should use Adobe Acrobat Reader which can be downloaded from: https://get.adobe.com/reader/

8) Clinical Data Management System / Electronic Data Capture – Requirements for Clinical Research Sites

Studies conducted for DAIDS are deployed using Electronic Data Capture (EDC) software. This software is also known as a Clinical Data Management System (CDMS). There are currently two different EDC systems used for DAIDS studies: DF/Net iDataFax and Medidata Rave. Both are web-based tools that allow the Clinical Research Site (CRS) to enter and interact with data and the Statistical Data Management Center (SDMC).

a) Minimum requirements for using web-based EDC:
   i) Client machine minimum requirements
      (1) Outbound port 443 (https) connectivity from client to the Internet.
      (2) 1 GHz or faster CPU and 2 GB RAM.
      (3) Windows or Mac OS, with up-to-date system updates.
      (4) HTML5-compliant browser such as Chrome, Edge, or Safari.
      (5) Printer or "print to PDF" capability for generating CRF hardcopies.
   ii) Process requirements

(1) EDC user account passwords should be rotated every 90 days and accounts must not be shared. Password rotation may be enforced by the SDMC.
(2) The CRS should identify a local IT contact to resolve connectivity/firewall issues.
(3) The CRS should identify a site primary contact that is responsible for managing users at the CRS and terminating accounts of any users who have departed within 30 days.
(4) Computers for EDC should be set up in a physically secure location.

9) LDMS lab requirements for trials using the Laboratory Data Management System (LDMS)

LDMS is offered as a Windows-based or Web-based program and allows for the electronic inventory and tracking of samples collected.

Windows Platform
Windows LDMS system requirements are found on the LDMS public website:
https://www.ldms.org/resources/ldms/windows/#intro/system-requirements.html

a) Minimum requirements: see Table 1. System requirements
b) Ideal requirements: see Table 2. System recommendations

Web Platform
Web LDMS system requirements are found on the LDMS public website:
https://www.ldms.org/resources/ldms/web/#intro/system-requirements.html

a) Minimum requirements: see Table 1. System requirements
b) Ideal requirements: see Table 2. System recommendations

Identifying and Recommending IT Infrastructure Standards

An established standard is nothing without conformance. As such, the "IT Best Practices Task Force" (ITBPTF), was formed to help identify similar expectations of minimum IT standards. This oversight body works with the sites to ensure that they are meeting the appropriate standard of IT infrastructure through the process of data-collection and site-assessment visits. The ITBPTF can consult the sites through shortcomings and work with them to reach the most-appropriate technological standard given their resource level and location.

Similarly, the ITBPTF will review and advise on prospective major changes to the base IT infrastructure of DAIDS-funded sites to prevent unforeseen technical conflicts that might result in the loss of services. Having the stakeholders represented in the decision-making process will facilitate communication, result in better-educated decisions, and minimize technical incompatibilities among heterogeneous technical systems.

Members of the ITBPTF will communicate via email listserv in an effort to keep each other appraised of technological matters as they arise. This can be used to share information in a timely manner, minimize the damage from outages, and generate cost efficiencies with travel and training.

Questions about the ITBP document and the standards established within can be sent to hancadmin@hanc.info.

Conclusion

"Information Technology Best Practice Standards at NIH HIV/AIDS Clinical Research Networks' Study Sites and Site Affiliated Laboratories" and the associated ITBPTF actions will ideally yield material results in the areas of data quality and operational efficiencies. As the effects of improved IT best practices accumulate over time, sites will be elevated to a greater level of operation and self-reliance, making them more efficient and productive with each network study.