August 2024 | APHL White Paper

Global Laboratory Data Security

A Guide to Ensuring Data Confidentiality, Integrity and Availability

Data security is a critical aspect of protecting sensitive information and assets at laboratories around the world, and the consequences of inadequate security practices can be devastating to public trust and reputation.

This document provides a high-level overview for laboratory directors, clinicians and other staff about how to limit unnecessary access to protected health information, with a focus on data confidentiality, integrity and availability.

APHL ASSOCIATION OF PUBLIC HEALTH LABORATORIES®

Contents

The Association of Public Health Laboratories (APHL) supports medical laboratories around the world, with a wide variety of information technology management oversight and governance approaches. Laboratories in different areas of management purview are subject to disparate policies and standards and face data security risks that, while not unique to laboratories, include threat and vulnerability pressures that are of particular concern to those responsible for laboratory data and information technology in a post-COVID-19 pandemic environment.

This paper provides a high-level overview of data security issues and associated risk management practices and guidance to laboratory directors, clinicians and various staff across the globe. This paper covers the key tenets of data security: data confidentiality, integrity and availability. It covers the importance of data security, risk factors of threat, vulnerability and the impact of threats exploiting vulnerabilities, as well as guidance for managing associated risks. This paper discusses backup and disaster recovery concepts, strategies and methods of designing and implementing a laboratory data backup capability.

What is Data Security?

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) define data security as "the preservation of data to guarantee availability, confidentiality and data integrity." This definition may be overly optimistic. Data confidentiality, integrity and availability cannot be guaranteed, and risks to other data attributes and the systems in which data are stored, processed and communicated are gaining significance. The authoritative US standard glossary of terms relating to information security created by the Committee on National Security Systems names the "prevention of damage to, protection of and restoration of computers, electronic communications systems, electronic communications services, wire communication and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and nonrepudiation" as "cybersecurity." The glossary makes no distinction between cybersecurity, data security, information assurance, etc., other than noting that they and related terms are sometimes used and attributed with subtle differences in meaning by organizations and communities that invoke them.

Laboratory data and information derived from data depend on controls in the information systems in which they are stored, processed and/or communicated. Information systems are comprised of more than hardware, software and data. Information systems include technology, people and processes that must be safeguarded to mitigate risks associated with a laboratory's use and reliance upon information technology (IT) through a risk management competency conceived, implemented, administered and overseen at the information system (IS)-owning organization's senior executive level.

Tenets of Data Security

It is important for laboratory leaders to understand some key concepts of data security: confidentiality, integrity and availability of laboratory data.

Data Confidentiality

The ISO defines confidentiality as a property that information is not made available or disclosed to unauthorized individuals, entities or processes. Data and information that have confidentiality concerns include user and process authentication information (e.g., passwords) and other information to which heightened sensitivity is assigned (e.g., personally identifiable information (PII)). PII is any information about an individual, including (a) any information that can be used to distinguish or trace an individual's identity such as name, social security number, date and place of birth, mother's maiden name or biometric records; and (b) any other information that is linked or linkable to an individual such as medical, educational, financial and employment information. Laboratories and other organizations that collect, process, store or communicate PII have legal and regulatory requirements to safeguard it in storage, during processing and transfer.

Factors that affect the need to maintain confidentiality of sensitive information, including PII, are quantity of information and data field sensitivity, or the degree of harm to individuals and organizations that could result from unauthorized disclosure of individual data elements and combined data elements. For example, an individual's name and government-issued identification number, medical history or financial account information is generally considered more sensitive than an individual's phone number or home address. Generally, data aggregations are of greater value to both the legitimate owners of the data and to adversaries because of the sum value and the heightened potential for new information to be derived from large data set analysis.

Threats to data confidentiality include malicious insider personnel and external human threats. Still, the greatest threat to data confidentiality within laboratory systems is from automated tools that may target specific organizations and data or, most commonly, self-propagating malicious code that targets indiscriminately, gains access to laboratory networks, and collects and absconds with pre-programmed types of sensitive information. Sensitive laboratory information is best safeguarded in transit and at rest when cryptographically protected. Similarly, sensitive information is most vulnerable when not encrypted, weakly encrypted, or strongly encrypted but paired with weak cryptographic key management or weak user authentication and access control.

Data Integrity

The ISO defines integrity as the property that data (or information systems) have not been altered or destroyed in an unauthorized manner. The first example of data integrity concerns may be unauthorized changes to data field values in database tables. This is a legitimate concern. A concern of greater significance may be changing process code elements that affect how an information system operates, how system event auditing is configured, reported or stored, or—even scarier—malicious changes to operating system kernels.

Monitoring system files for unauthorized changes is a fundamental data security capability and regulatory requirement. File integrity tools should be configured to detect and react to changes to operating systems, bootup/startup, password files, Windows Active Directory, databases, directories, kernel parameters, etc. Changes to be monitored may include file size, permissions, creation and modified dates, file contents, etc. Monitoring is generally accomplished by tools generating and comparing cryptographic hash values of files selected for monitoring. Data, system, network and enterprise-level encryption strategies are increasingly implemented as integrity attack countermeasures. Example file integrity monitoring (FIIM) tools include Tripwire by Fortra, CimTrak by CIMOR and EventLog Analyzer by ManageEngine.

Data Availability

The ISO defines availability as a property of data or resources being accessible and usable on demand by an authorized entity. Data and system unavailability may be either intentional or unintentional. Intentional unavailability may be due to scheduled downtime for maintenance. Most information systems' contingency plans allow for short downtime due to planned or unforeseen events before the unavailability event is considered an incident that requires notification or other response. Allowable downtime limits are determined during the business impact analysis (BIA) portion of contingency planning. When conducting a BIA, business processes supported by the system are identified and the effect of system disruptions on those processes is determined with outage impacts and estimated downtime. Business processes are ranked by criticality to enable restoration priorities. The downtime should reflect the maximum the laboratory can tolerate while still maintaining operations. Then, the resources required to perform identified processes and internal and external dependencies are identified. Priority levels can then be established for sequencing recovery activities and resources.

Laboratory systems and data may also be threatened by malicious denial of service attacks. Internet-connected systems may be specifically targeted by distributed denial of service (DDoS) attacks. The growing Internet of Things (IoT) and connected, special purpose laboratory equipment has led to a massive proliferation of network connectivity in traditionally not-connected objects and devices, many of which are insufficiently secured. Malicious actors have demonstrated their ability to compromise large numbers of these devices and other poorly protected computing endpoints, harnessing them in "botnets" to overwhelm Internet-connected targets with web traffic. The Center for Internet Security (CIS) recommends working with Internet service providers and companies providing DDoS mitigation services to help prevent and respond to DDoS attacks. CIS recommends organizations enable firewall logging of accepted and denied traffic to determine where the DDoS may originate and define strict "TCP keepalive" and "maximum connection" on all perimeter devices, such as firewalls and proxy servers. This recommendation assists with keeping most common "SYN Flood" attacks from being successful.

Ransomware attacks are another form of data availability attack to which medical organizations, including laboratories, are vulnerable. Ransomware is a scourge on the IT ecosystem and big business for cybercriminals. Ransomware infiltrates information systems and encrypts system data and the perpetrator extorts money from victims to regain access to victim data. Groups of hackers and veteran cybercriminals that develop ransomware software are increasingly "leasing" their software to other criminals—referred to as "ransomware as a service," or RaaS—who compromise targets, launch attacks and share a percentage of ransoms paid with the software owner. Most ransomware attacks begin with a phishing attack using fraudulent emails containing links that the victim clicks. The links engage malicious code that exploits vulnerabilities in applications such as Adobe Acrobat, Apple QuickTime and Microsoft Office to install malware on the target's system. Once installed, the malware program may extract data, search for specific documents, update itself, issue command and control functions, or encrypt data as part of a ransomware attack. Other sources of ransomware attack code include malicious websites, files downloaded from the Internet, connections over trusted networks to infected systems, files shared on USB flash drives or other removable media and compromised commercial software.

RaaS software has been known to gain an initial foothold by exploiting vulnerabilities and compromising accounts to access virtual desktop infrastructure that had been put in place to facilitate remote access during the COVID-19 pandemic.

The ransomware attackers establish command and control primarily with a Remote Desktop Protocol client running over port 443, routed through The Onion Router (TOR) software. After installing a TOR browser, they modify its configuration to run as a persistent service, redirecting traffic sent to a local (dynamic) port through TOR via HTTPS over port 443 so it would be indistinguishable from normal web traffic. The ransomware pivots and scans connected networks, runs commands, dumps processes and steals credentials to infiltrate targets and compromise Windows servers.

The best methods to safeguard laboratory systems from the ransomware threat is to:

- Educate laboratory system users about phishing—the exploit designed to compromise user accounts and privileges—and conduct phishing exercises to periodically test and strengthen user awareness.
- Implement the "Essential Eight" data security risk mitigating strategies discussed later in this paper.

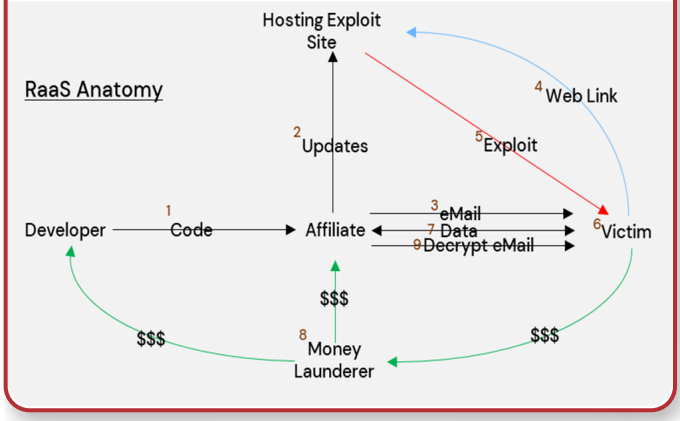
The ISO has added the tenets of non-repudiation and authenticity to the confidentiality, integrity and availability tenet triad and some organizations and communities have recently added information system resiliency. Non-repudiation is intended to assure that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. That assurance can significantly strengthen system event logging and auditing capabilities. Non-repudiation gained significance as a cybersecurity tenet with implementing public-key infrastructure (PKI)-based authentication and the widespread use of PKI tokens in the form of "smart card" credentials that strongly authenticate people. Similarly, the digital signature capability of PKI has the potential to significantly strengthen authentication assurance of data of all kinds, including documents, records, logs, etc.

Resiliency as a cybersecurity tenet is the ability of an information system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and recovering to an effective operational posture in a time frame consistent with business or mission needs. CMU SEI notes that to exhibit resilience, a system must incorporate controls that detect adverse events and conditions, respond appropriately to these disturbances and rapidly recover afterward. The availability of emerging security capabilities (e.g., public key technologies) contributes to enhanced attention to candidate cybersecurity tenets of non-repudiation and authenticity. In the case of resilience, the emergence of automated continuous monitoring and risk mitigation capabilities paired with machine learning and artificial intelligence promises of lightning-fast risk-mitigating response to threats, vulnerabilities and events has heightened expectations of organizations' abilities to design, implement and operate adverse event-resilient information systems.

Anatomy of RaaS

According to Carnegie Mellon University Software Engineering Institute:

1. The ransomware developer creates custom exploit code that is then licensed to a ransomware affiliate for a fee or share in proceeds from the attack.
2. The affiliate updates the hosting site with the custom exploit code.
3. The affiliate identifies and targets an infection vector and delivers the exploit code to the victim (e.g., via malicious email).
4. The victim clicks the link or goes to the website.
5. The ransomware is downloaded and executed on the victim's computer.
6. The ransomware encrypts the victim's files, identifies additional targets on the network, modifies system configurations to establish persistence, disrupts or destroys data backups and covers its tracks.
7. The victim receives a ransom note and is instructed to pay the ransom with untraceable funds, typically cryptocurrency.
8. A money launderer will move the money through multiple transformations to obscure the ransomware affiliate and developer's identities.
9. The ransomware affiliate may send a decryptor to the victim once a ransom payment has been received. The affiliate may make additional demands on the victim or do nothing at all and leave the victim with encrypted files.



Risk Management

Risk

Information technology risk is defined as a measure of the extent to which a potential circumstance or event threatens an entity and typically is a function of (i) the adverse impact or magnitude of the harm that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. The magnitude of risk factors (i.e., threat, vulnerability, impact and likelihood) and the risk they represent are most often expressed semi-qualitatively as a range of values (e.g., 0 to 100) to engage in an appropriate risk response and apply appropriate risk-mitigating countermeasures. Risk must be understood by laboratory leadership through the conduct of a risk assessment integrated into a risk management program.

Risk Assessment Methodology

The methodology described here is consistent with the US National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-30 Guide for Conducting Risk Assessments, as adapted and applied internationally by governments, academia and industry. The risk assessment methodology first evaluates and assigns semi-quantitative numerical values to the risk factors—threat, vulnerability, likelihood of threat exploitation of vulnerability—and the potential impact associated with successful exploitation.

Threats

Threat is defined as any circumstance or event with the potential to adversely impact organizational operations organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Threats are potential events, whereas an advanced persistent threat (APT) is an adversary. APTs have sophisticated levels of expertise and significant resources, allowing the use of multiple different attack vectors (e.g., cyber, physical and deception) to undermine critical aspects of a mission, program or organization, or place itself in a position to do so in the future. APTs pursue their objectives repeatedly over an extended time, adapting to defenders' efforts to counter them.

Adversarial attacks are characterized by the tactics, techniques and procedures (TTPs) employed. TTP identification and analysis are instrumental in APT identification and help organizations better understand what adversaries desire to gain through attacks and narrow the set of threat events that are most relevant to consider.

Potential Threats

Accidental Threats

- **Fire**
- **Electrical Disturbance**
- **Hardware Failure**
- **Environmental failure**
- **Operator Error**
- **User Error**
- **Configuration Error**
- **Software Error**
- **Accidental Disclosure**
- **Resource Consumption—Computer**
- **Telecommunication Interruption**

Intentional Threats

- **Alteration of Data**
- **Alteration of Software**
- **External Influence / Threat**
- **Vandalism**
- **Theft**
- **Intentional Disclosure**
- **Eavesdropping / Emanation**
- **Insider Penetration**
- **APT Penetration**
- **Malicious Code / Virus**
- **Resource Consumption**
  - **Computer**
  - **Telecomm**
- **Unauthorized Use of Resources**

Threats may be accidental or unintentional such as an act of nature (i.e., earthquake, flood, lightning) or intentional. Intentional threats are generally considered to be malicious—such as those represented by APTs and rogue insiders.

Surprisingly, threat and APT advisory reports rarely include severity metrics. To be incorporated into risk assessments, threat intelligence must be considered in the context of individual organization and system environment factors as part of a likelihood metric score. A subjective metric determination is recommended for the likelihood of a threat exploiting a vulnerability based on available evidence, experience and expert judgment. Combinations of factors such as threat targeting, intent and capability are used to produce a score representing the likelihood of threat initiation. The value ranges should be consistent with those used for vulnerability determination, as in the Common Vulnerability Scoring System (CVSS) range of 0-100.

Vulnerability

According to international standards, vulnerability is a known weakness in a system, system security procedures, internal controls or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify or disrupt normal operations of a system, resulting in a security incident.

Data security and privacy controls in laboratory systems are meant to prevent or counter vulnerabilities. Generally, vulnerabilities are associated with security controls that either have not been applied (either intentionally or unintentionally) or have been applied but retain some weakness. As new technologies are implemented and new threats emerge, new vulnerabilities not associated with existing controls or control descriptions found in standard control frameworks may be identified.

Types of Vulnerabilities

There are two general types of vulnerabilities: tactical (technical and physical) and strategic (IT governance, administrative and managerial).

Tactical/Technical Vulnerabilities

Most laypeople think of tactical areas—such as technical or physical aspects and controls—when considering laboratory data security vulnerabilities. These types of vulnerabilities are enumerated in the US National Vulnerability Database (NVD), which is relied upon throughout the world as an authoritative compilation of up-to date technical vulnerability information. Many vulnerability scanning tools test and report based on the contents of the NVD. Technical vulnerabilities include software coding weaknesses, hardware design flaws and weaknesses, system component misconfigurations and system component conflicts. The NVD defines vulnerability as:

> *A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, negatively impacts confidentiality, integrity or availability. Mitigating vulnerabilities in this context typically involves coding changes but could include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).*

CVSS Severity Scoring

Vulnerabilities are assigned severity scores to understand the issue's criticality and aid in risk calculations. The Common Vulnerability Scoring System (CVSS) leverages both versions 2.0 and 3.0 scales:

Severity	Score Ranges	
	CVSS V2.0	CVSS V3.0
None	–	0.0
Low	0.0 – 3.9	0.1 – 3.9
Medium	4.0 – 6.9	4.0 – 6.9
High	7.0 – 10.0	7.0 – 8.9
Critical	–	9.0 – 10.0

Common vulnerabilities and exposures (CVEs) are continually updated in the NVD as discovered and reported. They are very numerous. In January 2024 alone, 2,790 CVEs were received, analyzed and added to the NVD. Technical vulnerability scanning and malicious code detection tools must be continually updated to ensure that they identify newly reported CVEs. Technical controls typically receive the most attention but are generally of lesser potential impact significance than strategic, managerial and administrative IT governance vulnerabilities.

Strategic/IT Governance Vulnerabilities

Information systems (IS) are defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This is understood to mean that an IS includes hardware, software, data, cabling, devices, other technical components, people and processes. IT governance vulnerabilities are those related to people and processes. They include vulnerabilities relating to actions taken—or not taken—by people to manage the system's development, maintenance and use, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions. Technical controls are generally determined, implemented, configured, operated and maintained through a framework of IT governance controls. Technical vulnerabilities are frequently the result of IT governance vulnerabilities.

Root Cause Analysis

Data security at the system level is dependent upon commitment from senior level executive leadership. Strong executive leadership begets strong laboratory information systems management. Executive leadership directs and endorses data security policy for adoption and implementation of data security standards for laboratory systems risk management and data system control frameworks. Executive leadership directs human resources security programs including personnel assurance screening and data security training. Policies and standards define data and system owner responsibilities for data security including requirements for determinations of individual user access and other permissions and control of data sharing with external entities.

Technical vulnerabilities in laboratory environments almost always result from and may be traced back to strategic (administrative and managerial) control weaknesses in laboratory systems management or administrative infrastructure. Tactical weaknesses are occasionally caused by other tactical weaknesses that are, in turn, caused by strategic weaknesses. Consider the scenario in which systemic missing security patches on medical testing systems result from a malfunctioning automated patch management system because the individual who initially installed, configured and maintained it left the organization. The organization should have planned for such a contingency. In this example, automated scans identified the missing patch and assigned a vulnerability score, but the root cause is of much greater significance to associated risk as the faulty strategic control—ensuring continuity of necessary cybersecurity skills, knowledge, abilities and experience—will likely lead to other, widespread control weaknesses.

Because automated vulnerability scans and continuous monitoring and alerting systems typically identify defects at the tactical level, recognizing both root causes and the impacts of control failures is a critical capability. When significant systemic conclusions are reached and strategic control failures are identified, it may imply the need for new or modified governance controls (e.g., training of system administrators in a specific skill such as installing, configuring and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks). Policy changes, control requirements and related test and monitoring procedures for the new desired state specifications should then be established.

Adverse Impact

Impact represents the magnitude of harm expected if a threat exploits a vulnerability, resulting in loss of information or laboratory system confidentiality, integrity, or availability. Harm includes the potential impact on laboratory business objectives, organizational reputation, the performance of essential business functions and impact on individuals,

including physical and privacy harm. The processes used to make impact determinations are derived from strategic planning, policies and established business values. Sources to be considered may include BIAs used in continuity of operations and contingency planning, privacy impact assessments, etc.

Impact metric ranges should be on a level consistent with vulnerability and likelihood scores (e.g., 1-100).

Risk Metrics

The relationship between vulnerability, threat, potential impact, likelihood and criticality can be confusing. The risk value determination process in some standards includes many additional factors, including environmental, adversary capability, intent and targeting; it can be complex and difficult to understand and even more challenging to implement at the laboratory level.

For many years, the accepted risk determination calculation used in information security risk determination has been:

Risk = Impact x Threat x Vulnerability (R=ITV)

In this simple formula, if any of these risk factors is zero, the risk is also zero regardless of the other factors.

In risk computations, this fundamental relationship should be preserved. ISACA, an international professional association focused on IT governance, uses a simple process of:

Risk = Criticality (Likelihood × Vulnerability Scores) × Impact

If medical laboratory organizations standardize on the CVSS v3.0 metric range of 0-100 for risk factors and assign risk scores to each factor of None (0), Low (1), Medium (2), High (3) and Critical (4), risk calculation becomes very simple and is based on a range from 0 to a possible highest score of 64 ([4 X 4] X 4). A semi-qualitative risk determination may be made using this scale.

Criticality Score	Impact Score			
	1	2	3	4
1	L	L	L	L
2	L	L	L	L
3	L	L	L	L
4	L	L	L	M
5	L	L	L	M
6	L	M	M	M
8	M	M	M	M
9	M	M	M	M
10	M	M	M	H
12	M	M	H	H
15	M	M	H	H
16	M	H	H	H
20	H	H	H	C
25	H	C	C	C

Periodic System-level Risk Assessments

At the laboratory system level, risk management frameworks include threat, vulnerability and risk assessments to be performed before going live with any significant change to the system—from initial startup to those changes occurring through the system life cycle that may be expected to affect the system's control environment.

Program-level Risk Assessments

In part, laboratory organizational risk assessments are used to inform the security and privacy control selection process. The selection process results in an agreed-upon set of security and privacy controls addressing specific mission or business needs consistent with organizational risk tolerance. Regulatory standards generally require periodic control audits to be performed by or under the authority of internal audit competencies; publicly traded corporations require periodic external audits of the IT control environments to be conducted by independent third parties and require threat, vulnerability, impact and risk assessments to be performed.

Risk Assessment Upon Receipt of Threat/ Vulnerability Intelligence

The system or organization's data security monitoring competency should perform a risk assessment upon receipt of new threat or vulnerability information—whether from the organization's own monitoring capabilities or from external sources. If the risk score and organizational policy require, based on established risk tolerance, a change request associated with the risk (which may or may not reflect the recommendations in the original advisory) to enter the system or organization's system engineering lifecycle where additional evaluations occur, risk mitigating countermeasures are developed or refined, tested, implemented and documented in concert with other steps, competencies and functions of the system engineering and risk management frameworks.

Laboratory Applications for Data Security

Security Requirements

Data security requirements are protection needs and/or obligations prescribed by laboratory organizational policy and regulatory authorities, laws, orders, directives, standards, business needs or risk assessments. Requirements prescribe capabilities that laboratory organizations and systems must meet, and may include:

Access Control: Laboratory organizations must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and the types of transactions and functions authorized users are permitted to exercise.

Contingency Planning: Laboratory organizations must establish, maintain and effectively implement plans for emergency response, backup operations and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergencies.

Planning: Laboratory organizations must develop, document, periodically update and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Physical and Environmental Protection: Laboratory organizations must:

- Limit physical access to laboratory information systems, equipment and the respective operating environments to authorized individuals.
- Protect the physical plant and support infrastructure for information systems.
- Provide supporting utilities for information systems.
- Protect information systems against environmental hazards.
- Provide appropriate environmental controls in facilities containing information systems.

Security Controls

Controls are the mechanisms by which organizations, systems and administrative infrastructure implement requirements. In ISO 12812-1:2017, the ISOs define the term “security controls” to be management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. One may infer that physical and environmental controls are included under this definition.

The 1993 British Standard, BS7799 is the foundation of modern control frameworks that spawned the ISO/IEC 27000 series as well as NIST SP 800-53, *Security and Privacy Controls for Systems and Organizations*, a catalog of over 1000 controls arranged in 19 control families from which organizations select to meet requirements. Its companion publication, 800-53B, provides default sets of baseline controls for low, moderate and high levels of assurance. This standard and derivatives of it are used worldwide by all types of IT-dependent organizations including medical laboratories.

These frameworks offer similar administrative, physical and technical security and privacy control options to safeguard the confidentiality, integrity and availability of data, information and associated information systems.

Control Objectives for Information and Related Technologies (CObIT) was first released in 1996 by the international professional association ISACA as a set of control objectives to aid the financial auditing community in working more effectively with IT-related structures. Unlike BS7799 derivatives, CObIT—now simply "COBIT"—provides a control framework that looks beyond conventional data security to include the control tenets of effectiveness, efficiency, compliance and reliability as broader IT governance objectives.

The risk management methods for determining, designing and implementing appropriate data security controls are no different for medical laboratories than they are for any other IT-dependent organization. However, medical laboratories do have heightened concerns for in-common vulnerabilities that emphasize needs for risk-mitigation controls.

Vulnerabilities and Risks of Special Concern

Below are examples of vulnerabilities that may be of concern:

- Laboratories in African countries face heightened risk from threats and vulnerabilities systemic to the continent. A 2021 Interpol Cyberthreat Assessment report on African Cybercrime reports that 60% of the population in Africa is under 25 years old, which the report concludes is driving rapid growth in the use of new and innovative information technologies. That, combined with the effects of the COVID-19 pandemic on loss of jobs and reduced economic growth, has increased opportunities for cybercrime, including money laundering, transnational crime and cyberextortion (ransomware crime, in particular). Interpol reports that in 2020 alone, over 61% of African companies were affected by ransomware and healthcare was called out as a particularly favored target of ransomware cybercriminals.
- COVID-19 also affected medical and laboratory device deployment timelines and reduced the supply chain time frames from months or years to days or weeks to meet testing and treatment needs of newly stay-at-home and quarantining populations. The pressures caused short-cutting in cybersecurity risk-mitigating regulatory and policy compliance, resulting in a target-rich, vulnerable ecosystem of medical devices and systems. That compounded risks posed by special-purpose medical equipment known for embedded software and operating systems that are either beyond end-of-life support for security updates and patches or otherwise outside of the laboratory IT configuration management control.
- Although the US, European Union and other countries have regulations and third-party assessment requirements for medical device security and safety, the United Kingdom's National Biomedical Engineering reported in 2020 that start-ups often drive innovation in the medical sector; these small companies often have great ideas but lack the understanding and wherewithal to identify and comply with security regulations. Biomedical engineers in start-ups may treat security requirements as "user story" capabilities deferred to later builds—builds that may never happen. Medical equipment producers are increasingly enabling Wi-Fi or other wireless protocols in medical laboratory devices to enhance usability, communication and software maintenance automation, making them vulnerable to automated malicious code targeting Internet-of-things devices.
- Public health laboratories continually receive input source data from hospitals, clinics and/or healthcare providers. More advanced laboratories on-board connected sources with application programming interfaces (API) using encrypted virtual private networks (VPN) across the public Internet. As part of the on-boarding, the explicit data format, metadata and the use of a unique encrypted source identifier are defined through a data use agreement (DUA). These unique identifiers are decrypted on the receiving end and validated as being from the expected source. At a minimum, if an encrypted identifier is not used, the data source is validated from the expected source by the VPN endpoints.
- In less sophisticated health data sources or laboratories, the data delivery method may consist of uploading to a password-protected web portal. Multi-factor authentication (MFA) should be used with all user accounts accessing the web portal. The portal must be configured for HTTPS for secure communication over computer networks, particularly the Internet. HTTPS encrypts data transmitted between web browsers and websites, thus providing confidentiality and integrity for sensitive information exchanged between the user's device and the web server. Communication between public health laboratories, community health programs, government or national health departments, or Ministries of Health would follow similar processes using APIs or Secure Web Portal transfer data.

Interconnection Security Agreements

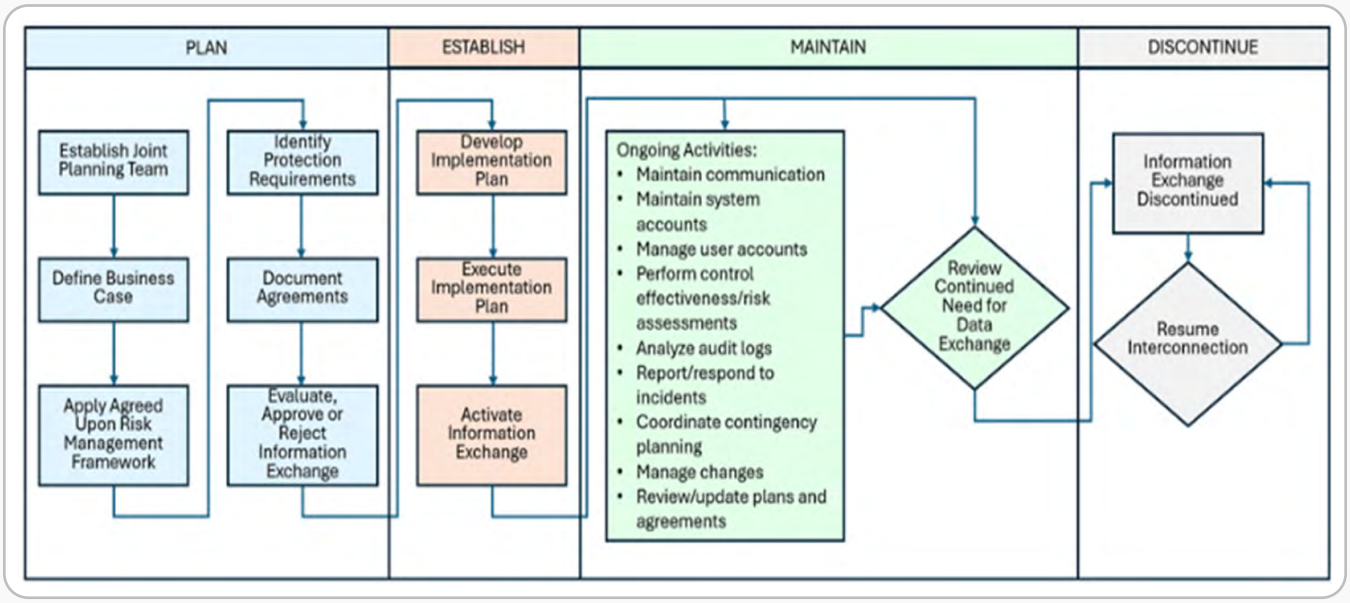
Interconnection security agreements and memorandum of understanding provide partners with the parameters in which the data can be used and how it can be accessed. Such documents are authorized by the senior officials with data security responsibility in the exchanging organizations and typically address:

- Level and method of interconnection
- Impact on existing infrastructure and operations
- Hardware requirements
- Software requirements
- Data sensitivity
- User community
- Services and applications
- Security controls
- Segregation of duties
- Incident reporting and response
- Contingency planning
- Data element naming and ownership
- Data backup
- Change management
- Rules of behavior
- Security awareness and training
- Roles and responsibilities
- Scheduling
- Costs and budgeting

Interconnection Agreement Management: NIST Special Publication 800-47

NIST Special Publication 800-47 **is an internationally recognized and widely implemented guide for managing the security of exchanges of information between organizations. It prescribes interconnection security agreements between organizations operating under different governance control involved in information exchanges.**

Life-Cycle Phases of Information Exchange Management



Essential Eight: Data Security Risk Mitigating Strategies

1. Patch Applications

- Automate scannable asset detection.
- Implement application vulnerability scanning using up to date vulnerability database.
- Scan office productivity suites, web browsers and their extensions, email clients, PDF software flash players and security products at least weekly for missing patches/vulnerabilities.

2. Patch Operating Systems

- Automate scannable asset detection.
- Scan Internet-facing servers and devices daily.
- Scan non-Internet-facing servers and devices at least twice/month.
- Apply patches within 48 hours of release for critical vulnerabilities within two weeks for non-critical vulnerabilities if no know working exploits are available.
- Replace operating system that are unsupported, beyond end of life.

3. Implement Multi-factor Authentication

Use MFA to authenticate users:

- That access sensitive laboratory data
- From third-party services that process sensitive laboratory data
- For online customer services that process sensitive laboratory data.

4. Restrict Administrative Privileges

- Validate requests for privileged access to systems, applications and data repositories.
- Privileged users must only use dedicated accounts for privileged access; never use same accounts for privileged and non-privileged access.
- Limit privileges to minimum required to perform functions.

5. Application Control

- Implement on workstations and apply to user profiles and temp folders used by operating systems browsers and email clients.
- Restrict executables, software libraries, installers compiled HTML, HTML applications and control panel applets to an approved set.

6. Restrict Microsoft Office Macros

- Disable macros for users that do not have a demonstrated business requirement.
- Block macros in files originating from the Internet.
- Deactivate users' ability to change Microsoft Office macro security settings.

7. Harden User Authentication

- Disabled or remove Internet Explorer 11.
- Block ability for browsers to process Java from the Internet.
- Block ability for browsers to process web advertising from the Internet
- Deactivate users' ability to change browser security settings.

8. Perform Regular Backups

- Perform and retain backups of data, applications and settings in a secure and resilient manner.
- Synchronize backups of data, applications and settings to enable restoration to a common point in time.
- Ensure unprivileged accounts cannot access backups belonging to other accounts and cannot modify or delete backups.

Countering Biomedical Laboratory Data Security Risk

Regional socioeconomic threats and vulnerabilities to medical laboratories are best countered by implementing and enforcing strong regulatory governance and oversight requiring standardization on internationally recognized data security requirements, methods and frameworks for information risk management and control. Regulatory requirements for standards implementation should include organization-level data security policy and independent verification and validation of compliance. Internationally accepted frameworks include requirements and methods for strengthening supply chain risk management through control of laboratory hardware, software and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of laboratory systems and system components.

Strong configuration management of acquired IT resources is also critical for the biomedical sector. Laboratory organizations should document all systems, hardware and software under their control. The organization should standardize configuration of software and devices on evaluated and approved security baselines. Changes from baselines should be formally assessed and approved. Special-purpose equipment containing embedded software and operating systems should be documented, managed and continually evaluated for security vulnerabilities.

Laboratories and their governance authorities should implement controls from established catalogs using recognized risk management frameworks. Some laboratories' data security maturity level or organizational size may not support a fully developed data security program. For those laboratories and at a minimum, the most basic controls should be designed, implemented, tested and approved at both the system and organization level. The Australian Signals Directorate produced what they call the "Essential Eight" data security risk mitigating strategies that are exceptionally well suited for consideration by biomedical laboratories lacking sufficient administrative infrastructure to immediately undertake full scope data security programs.

Information Systems User Best Practices

Internationally accepted frameworks and standards for data security control include organization-level information security policy. A core element of organizational information security policy is a "roles and responsibilities" section. The information security roles defined within organizations' policy may differ widely and include C-suite executives and other senior officials, information system security managers, security officers, privacy officers, security engineers, system and data owners, and mission owners, along with different roles and titles.

Typically, system owners are ultimately responsible for the security of their systems and ensuring system-level controls are appropriately designed, implemented correctly and operating effectively. System-level security officers (sometimes filled by security administrators) generally review and approve access requests, or that responsibility may be assigned to the data owner. A role that every organizational cybersecurity policy will almost certainly include is that of the end user of the organization's information systems. The "system user" role is an individual or process acting on behalf of an individual authorized to access information and information systems to perform assigned duties. System user responsibilities include, but are not limited to, adhering to policies that govern acceptable use of organizational systems. User policies differ, but some common and appropriate behavioral guidelines for all users of organizational information technology include:

- Never attempt to access systems to which access has not been authorized.
- Protect passwords and other authenticators from disclosure; never share passwords with anyone, including system administrators.
- Never record passwords on paper or in electronic form.
- Promptly change passwords whenever compromise is suspected.
- Never attempt to bypass access control measures.

- Protect sensitive information from disclosure to unauthorized persons or groups.
- Only share information from organization-owned systems in accordance with privacy, legal, security and policy requirements.
- Lock user workstations or laptop computers or use password-protected screensavers whenever they are away from the work area.
- Never install any unauthorized software on organization-owned systems.
- Only use organization-owned systems for access to personal e-mail as permitted by organization policy.
- Never use unauthorized cloud services or peer-to-peer (P2P) file sharing to connect remotely to other systems to share files.
- Never open any links contained in an email unless the sender and source are known, the email is expected and verified through an out-of-band process (e.g., phone or Internet look-up).
- Follow security practices that are equivalent to those required at the primary workplace when working remotely.
- When not in use, physically protect any communications and computing equipment used for teleworking.

Backups and Disaster Recovery

Critical Components

Backup and disaster recovery (DR) are critical components of any public health laboratory organization's IT infrastructure management strategy. They are closely related but serve distinct purposes:

Backup: Making copies of data and storing them in a separate location or medium. The primary purpose of backups is to protect against data loss caused by accidental deletion, corruption, hardware failure or other unforeseen events.

Disaster recovery: Processes and procedures for restoring laboratory IT infrastructure and data after a catastrophic event or disruption, such as a natural disaster, cyberattack, hardware failure or human error. The goal of DR is to minimize downtime, recover data and systems and restore normal operations as quickly as possible following a disaster.

Developing a Backup Strategy

Developing a robust backup strategy and feature sets is essential to protect critical data assets, minimize the risk of data loss and ensure business continuity during disruptions or disasters.

- **Identify and assess data and risks:** Identify and understand the laboratory data sources that need to be backed up. Determine how each data source will be backed up and whether any specialized backup methods or agents are required. Assess potential risks and threats to your data, such as hardware failures, software errors, cyberattacks, natural disasters and human errors.
- **Define recovery objectives:** Establish recovery objectives, including recovery point objectives (RPOs) and recovery time objectives (RTOs), to determine how much data loss and downtime your laboratory organization can tolerate.
- **Select backup solutions:** Choose backup solutions that align with your organization's needs, budget and IT infrastructure.
- **Determine backup frequency:** When scheduling backups, consider data criticality, change rates, business hours, recovery objectives and peak usage times to minimize disruption to operations.

- **Select backup methods:** Configure appropriate backup settings such as backup type (i.e., full, incremental, differential and snapshots), compression and encryption.
- **Define storage and retention policies:** Determine where backup data will be stored. Establish retention policies to manage backup storage duration and capacity.
- **Implement security measures:** Implement security measures to protect backup data against unauthorized access, tampering and data breaches. Encrypt backup data both during transmission and at rest to safeguard sensitive information.
- **Automate backup processes:** Use backup software or scripts to automate backup tasks, scheduling, monitoring and reporting. Set up alerts and notifications to alert administrators of backup failures, errors, or issues that require attention.
- **Test and validate backups:** Regularly test and validate that backup and recovery processes are performed correctly to ensure they meet recovery objectives and work as expected.
- **Document and review backup strategy:** Maintain up-to-date documentation, including backup schedules, settings, recovery procedures and contact information for support to compliance audits and training for personnel responsible for managing backups to ensure they understand best practices, procedures and tools.

Overall, a comprehensive backup and DR strategy is essential for mitigating risks, ensuring business continuity and protecting laboratories against data loss and downtime caused by unexpected events. Laboratory organizations should regularly review and update their backup and DR plans to adapt to threats and business requirements.

Key Considerations

- **Recovery Point Objective:** Maximum acceptable amount of laboratory data loss the laboratory is willing to tolerate during a disruption or disaster. This determines the frequency of backups.
- **Recovery Time Objective:** Maximum acceptable downtime or outage duration the laboratory organization is willing to tolerate for its critical systems, applications or business processes during a disruption or disaster. It determines how quickly systems and data must be recovered after a disruption or disaster.
- **Backup storage and retention:** Backups should be stored securely in an off-site location to protect against localized disasters.
- **Backup testing:** Regular testing of backups and DR plans is crucial to ensure that laboratory systems and data can be restored successfully and systems can be recovered within the required time frames.
- **Automation and monitoring:** Automated backup processes and monitoring tools help ensure that backups are performed consistently and that any issues or failures are detected promptly.
- **Data encryption and security:** To protect sensitive information from unauthorized access and data breaches, backups should be encrypted, sensitive data should be protected and unauthorized access should be prevented, regardless of the media used. Use Encryption methods such as AES (Advanced Encryption Standard) to encrypt backup files during transmission and at rest, thus adding an extra layer of security to your backup strategy, especially when storing backups in the cloud or on portable storage devices.

Key Decisions

3-2-1 Backup Strategy

The 3-2-1 backup strategy is adaptable to various laboratory environments and storage options, allowing laboratory organizations to tailor their backup solutions to their specific needs and available resources. It is a widely recommended best practice approach to data backup that provides redundancy and resilience against data loss due to various scenarios, including hardware failures, accidental deletions, cyberattacks and natural disasters. By following the 3-2-1 backup strategy, laboratory organizations can significantly enhance their data protection capabilities and minimize the risk of data loss, ensuring business continuity and data integrity.

- **Three copies of data:** Original data plus two additional backup copies. With three copies of data, there are multiple layers of redundancy, reducing the risk of data loss. The third copy is generally a replica or mirror of the backup copies on site and is used to minimize the RTO vs retrieving off-site tapes from a provider.
- **Two different storage media:** Storing backup copies on two different types of storage media. This could include a combination of internal hard drives, external hard drives, network-attached storage (NAS), tape drives, virtual tape libraries (VTL), cloud storage, or optical media (e.g., DVDs). Storing backup copies on different types of storage media helps protect against failures or vulnerabilities specific to a single medium.
- **One off-site backup:** Keep at least one backup copy off-site, preferably in a geographically distant location from the primary data source. Off-site backups ensure data can be recovered even in a catastrophic failure or disaster affecting the primary data location, such as fires, floods, earthquakes, or theft. If the laboratory or governmental authority considers using a cloud storage service, they must ensure that the provider adheres to all local country sovereignty regulations (e.g., within the country's borders).

Determining Backup Frequencies

Depending on the data and software environment's criticality, backups should be performed regularly to ensure that data is up-to-date and readily available for restoration when needed. Different backup methods include full backups (e.g., copying all data), incremental backups (e.g., copying only changed data since the last backup) and differential backups (e.g., copying changed data since the previous full backup).

Determine how often you'll perform backups (e.g., daily, weekly, monthly) and set up automated backup tasks to ensure consistency and reliability.

Laboratory IT organizations must assess their specific requirements, data sensitivity, compliance obligations and recovery objectives. Regular testing, monitoring and validation of backup processes are also critical to ensure data resilience and readiness for recovery in case of data loss or disasters.

Schedule backups during off-peak hours to minimize system resource usage and disruption.

The following are best practice backup frequency recommendations for laboratory software environments.

Daily or Multiple Times Daily (e.g., hourly) Backups

Production (Prod) environment: Data in Prod environments are subject to frequent updates, transactions and interactions, making frequent backups essential for data protection, disaster recovery and business continuity. Backup frequencies may, but daily or multiple times daily backups (e.g., hourly) are typically recommended for Prod environments.

Daily or Weekly Backups

Development (Dev) environment: While data in dev environments may change frequently, the focus is often on code and configuration management rather than data persistence.

Testing (Test)environment: Data in test environments may change less frequently than in dev environments but is still subject to updates, tests and modifications.

Staging (Stage) environment: Stage environments serve as pre-production environments where laboratory systems and software changes are validated, reviewed and staged before deployment to production. Data in stage environments may closely resemble production data and configurations, making backups critical for ensuring data integrity and recoverability.

Weekly / As Needed Backups

Training environment: While data in training environments may not change frequently, regular backups are still important for preserving training materials, user progress and customizations.

Determine Backup Types

Incremental and differential backups are two types of backup strategies used in data protection to capture changes made to data over time.

- **Incremental backup:** Incremental backups capture only the data that have changed since the last backup, whether full or incremental. Incremental backups are typically smaller, require less storage space and are faster to perform than full backups.

  To restore data from incremental backups, however, you must restore the latest full backup followed by all incremental backups to bring the data up to the desired recovery point, thus increasing the complexity of the restore process.

- **Differential backup:** Differential backups capture only the data that have changed since the last full backup. Each differential backup contains all changes made since the previous full backup, regardless of when it was performed. Differential backups capture all changes made since the previous full backup, making them larger compared to incremental backups.

  To restore data from differential backups, you only need restore the latest full backup followed by the most recent differential backup. The number of differential backups remains relatively small, reducing the complexity of the restore process.

Each approach has advantages and trade-offs in terms of storage requirements, backup and restore speeds and complexity of the restore process. Laboratory organizations should choose the backup strategy that best aligns with their data protection requirements, recovery objectives and resource constraints.

- **Database backup:** Database backup is critical to database management to protect data integrity, ensure laboratory business continuity and enable disaster recovery. Establish a backup schedule based on your data recovery objectives, business needs and compliance requirements.

  RPO can be everything from real-time (requiring a Business Continuity solution) to 24-hour (covered under daily backups). To meet RTO requirements, automated processes copy the database transaction logs to a secondary location at the required frequency. With this process, a database can be restored with the last full (or replicated) backup and then run the transaction logs forward to when the log was last copied.

- **File backup:** File backup is creating duplicate copies of files and storing them in a separate location to protect against data loss, corruption, or accidental deletion.

Backup Strategy

- **Select backup software:** Choose backup software that suits your preferences, encryption capabilities and operating system. Gartner publishes a Magic Quadrant for Enterprise Backup and Recovery Software Solutions, providing a good starting point. It is generally recommended that each laboratory utilize the same software to improve purchasing power and common and interchangeably trained staff.

- **Perform initial backup:** Perform an initial backup to create a baseline copy of your files. This initial backup may take some time to complete.

- **Regularly update backups:** Perform regular backups according to your backup and retention schedules to keep your backups updated.

- **Verify backup integrity:** Verify the integrity and completeness of your backups regularly to ensure that they can be restored successfully when needed. The best practice recommendation is to perform test restores semi-annually but no longer than annually.

- **Implement retention policies:** Laboratory organizations should choose the backup strategy that best aligns with their data protection requirements, recovery objectives and resource constraints. Based on regulatory requirements, business needs and laboratory data recovery objectives, retain backups for a specified duration. Rotate or archive backups to free up storage space and maintain compliance.

  Each backup and retention approach has advantages and trade-offs in terms of storage requirements, backup and restore speeds and complexity of the restore process.

  Considering today's tape capacities and compression technologies, the best practice recommendation is to use a weekly full backup with daily differential backups for six days. This process should continue for five weeks, then recycle the oldest weekly and daily backups. If the RTO allows for remote retrieval time, only the current and previous weeks are recommended to remain on site and all older backups are rotated off-site.

  The fifth weekly backup is retained for the monthly. These are kept for 12 months, then rotated; the last is kept as the yearly archive.

- **Monitor backup operations:** Monitor backup operations regularly to ensure backups are completed successfully and within the specified time frame. Set up alerts and notifications to notify administrators of backup failures, errors, or issues that require attention.

- **Store backups off-site:** Off-site backups provide additional redundancy and ensure your data is safe even if your primary backup location is compromised.

- **Document backup procedures:** Document your backup procedures, schedules, configurations and recovery processes in detail.

Data Sovereignty

Data sovereignty requires careful consideration and management by laboratory organizations operating in a global and interconnected world. It refers to the concept that data is subject to the laws and regulations of the country or jurisdiction in which it is located or processed. Laboratory organizations can mitigate legal and compliance risks by understanding and addressing data sovereignty requirements, protecting data privacy and security and building trust with healthcare and laboratory partners, regulators and the public. Data sovereignty should be covered in a data use agreement (DUA) between the healthcare providers, regional and national laboratories and well as country Ministries of Health. A DUA may include:

- **Legal and regulatory compliance:** Data sovereignty defines laboratory requirements of the jurisdictions in which they operate or store data. This includes data privacy, security, retention and cross-border data transfer laws.
- **Data localization:** Data localization laws aim to protect sensitive data, promote data privacy and ensure government access to data for legal or regulatory purposes.
- **Cross-border data transfers:** For jurisdictions with strict data protection laws, Laboratory organizations must ensure cross-border data transfers comply with applicable regulations, such as obtaining consent, implementing appropriate safeguards and using approved transfer mechanisms.
- **Cloud computing and outsourcing:** Cloud computing and outsourcing arrangements can raise challenges related to data sovereignty, as data may be stored or processed in multiple jurisdictions by third-party providers. To ensure compliance, laboratory organizations must carefully assess data sovereignty risks and requirements when engaging cloud service providers or outsourcing data processing activities.
- **Risk management:** Laboratory organizations must identify, assess and mitigate risks related to data sovereignty to avoid legal, financial and reputational consequences associated with non-compliance.
- **Contractual obligations:** Laboratory organizations address data sovereignty requirements through contractual agreements with third-party service providers. Contracts may include provisions related to data storage location, data access, data protection measures and compliance with applicable laws and regulations.
- **Data governance:** Laboratory organizations must establish data governance policies, procedures and controls to govern data collection, storage, processing and sharing activities in accordance with legal and regulatory requirements.

References

1. Australian Cyber Security Centre. (n.d.). Essential Eight Explained. Retrieved from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
2. Ben-Menahem, S.M., Nistor-Gallo, R., Macia, G., von Krogh, G., & Goldhahn, J. (2020). How the new European regulation on medical devices will affect innovation. Nature Biomedical Engineering, 4, 585–590.
3. Carnegie Mellon University Software Engineering Institute. (n.d.). Retrieved from https://www.sei.cmu.edu/
4. Center for Internet Security. (n.d.). CIS Controls. Retrieved from https://www.cisecurity.org/controls
5. Gartner. (n.d.). Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions. Retrieved from https://www.gartner.com/en/documents/4003661
6. Interpol. (2021). INTERPOL report identifies top cyberthreats in Africa. Retrieved from https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa
7. ISO. (n.d.). ISO 59844. Retrieved from https://www.iso.org/standard/59844.html
8. National Institute of Standards and Technology. (n.d.). NIST Special Publication 800-47 (Revision 1): Managing Information Security Risk: Organization, Mission and Information System View. Retrieved from https://csrc.nist.gov/pubs/sp/800/47/r1/final
9. National Institute of Standards and Technology. (n.d.). Glossary. Retrieved from https://www.cnss.gov/CNSS/openDoc.

Association of Public Health Laboratories

The Association of Public Health Laboratories (APHL) works to strengthen laboratory systems serving the public's health in the US and globally. APHL's member laboratories protect the public's health by monitoring and detecting infectious and foodborne diseases, environmental contaminants, terrorist agents, genetic disorders in newborns and other diverse health threats.

7700 Wisconsin Avenue, Suite 1000 Bethesda, MD 20814 | 240.485.2745 | www.aphl.org

This project was 100% funded with federal funds, supported by Cooperative Agreement #NU2HGH00080 from the US Centers for Disease Control and Prevention (CDC). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of CDC.