J Pathol Inform

Review Article

Privacy and security of patient data in the pathology laboratory

Ioan C. Cucoranu, Anil V. Parwani, Andrew J. West[1], Gonzalo Romero-Lauro[1], Kevin Nauman[1], Alexis B. Carter[2], Ulysses J. Balis[3], Mark J. Tuthill[4], Liron Pantanowitz

Departments of Pathology, University of Pittsburgh Medical Center, Pittsburgh, PA, [1]Pathology, University of Pittsburgh Medical Center, Information Services Division, Pittsburgh, PA, [2]Pathology and Laboratory Medicine and Biomedical Informatics, Emory University School of Medicine, Atlanta, GA, [3]Pathology, University of Michigan, Ann Arbor, MI, [4]Pathology and Laboratory Medicine, Division of Pathology Informatics, Henry Ford Hospital, Detroit, MI

E-mail: *Ioan C. Cucoranu - cucoranuic@upmc.edu
*Corresponding author

Received: 27 December 12 Accepted: 5 February 13 Published: 14 March 13

This article may be cited as:
Cucoranu IC, Parwani AV, West AJ, Romero-Lauro G, Nauman K, Carter AB, *et al.* Privacy and security of patient data in the pathology laboratory. J Pathol Inform 2013;4:4.

Available FREE in open access from: http://www.jpathinformatics.org/text.asp?2013/4/1/4/108542

Abstract

Data protection and security are critical components of routine pathology practice because laboratories are legally required to securely store and transmit electronic patient data. With increasing connectivity of information systems, laboratory work-stations, and instruments themselves to the Internet, the demand to continuously protect and secure laboratory information can become a daunting task. This review addresses informatics security issues in the pathology laboratory related to passwords, biometric devices, data encryption, internet security, virtual private networks, firewalls, anti-viral software, and emergency security situations, as well as the potential impact that newer technologies such as mobile devices have on the privacy and security of electronic protected health information (ePHI). In the United States, the Health Insurance Portability and Accountability Act (HIPAA) govern the privacy and protection of medical information and health records. The HIPAA security standards final rule mandate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. Importantly, security failures often lead to privacy breaches, invoking the HIPAA privacy rule as well. Therefore, this review also highlights key aspects of HIPAA and its impact on the pathology laboratory in the United States.

Key words: Antivirus, audit, biometrics, data backup, data integrity, encryption, firewall, health insurance portability and accountability act, internet, password, privacy, security, spyware, virtual private networks

Access this article online
Website:
www.jpathinformatics.org
DOI: 10.4103/2153-3539.108542
Quick Response Code:

INTRODUCTION

The protection of computer equipment, data, information, and computer services from unintended or unauthorized access, unplanned events, and even physical destruction is vital for any individual or organization that uses computers. Threats to computers and electronic information can be caused by humans intentionally (e.g., security breach, hackers activities, malware) or unintentionally (human error), by technology failures (e.g., system crash, down-time, firmware version inconsistencies) or environmental hazards (e.g., power surge, computer room fire, water leaks from defective sprinklers, heating, ventilation and air conditioning (HVAC) plumbing, effluent back-flow into sub-floors, natural disasters, etc.) Data protection and security are critical components of daily pathology practice that impact the entire information technology (IT) infrastructure including individual workstations, servers, and networks.

With increasing connectivity of information systems, laboratory instruments, work-stations, and mobile devices to the Internet and wireless networks, the demand to continuously protect data in all of its forms, locations and transmissions can become a daunting task. The responsibility of assuring that patient data in the pathology laboratory remains private and secure rests with the pathology informaticists, ideally working closely with their information services division. Therefore, it is important that informaticists are knowledgeable about security threats and privacy regulations that impact the pathology laboratory, as well as candidate technological solutions available to address them.

It is equally important that the laboratory's overall IT infrastructure be incorporated in recovery strategies developed for IT systems, applications and data, ideally in a manner that mirrors the standard practices already in use by the greater enterprise, thus supporting economies of scale and standard work. In this review, we introduce the reader to key technical terms and processes related to data security as it pertains to the laboratory information system (LIS), provide our insight into current and future challenges related to securing health-care data with rapid technological changes, and describe current regulations in the USA related to patient data privacy and security. Table 1 provides a glossary of common terms related to data privacy and security.

Table 2 presents topics discussed in this review (mainly data protection, privacy, security, and availability) organized in relation to the potential threats described above:

1. Disasters: Management of information systems to guard against, and enable response to, disasters and catastrophe (environmental, technological or human error).
2. Security Breaches: Protection against malicious intrusion or data theft, and recovery from security breaches.
3. Privacy and data management for research.

LABORATORY DATA SECURITY POLICIES AND PROCEDURES

Pathology laboratory workflow is dependent on the use of LIS, which acquires, generates, analyzes, stores, and manages electronic protected health information (ePHI). In addition to LIS, laboratories likely also store ePHI in software that run laboratory instruments and automation lines as well as in middleware such as auto-verification software. Therefore, making sure that the data contained in laboratory software remain protected and secure at all times is critical to daily pathology practice.[1] The same is true for interfaced devices such as chemistry analyzers that also store ePHI. Accordingly, security policies and procedures have to be in place and enforced in the laboratory.

In US laboratories, security must meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) (see the US Regulations for Health Information Security section), while other countries have developed similar security regulations for patient data. Major security elements that should be addressed include prevention of unauthorized access to patient's medical records (confidentiality), prevention of unauthorized alterations or loss to data (integrity), and prevention of compromises to availability of data to authorized individuals. Hence, incomplete or unavailable data is not considered secure.[2] In order to develop an effective security program, security measures must be designed to allow authorized end-users access to information in a timely manner.[3]

The ultimate responsibility for security implementation and compliance belongs to the health-care entity that manages data. A security risk analysis is a systematic process designed to examine and identify any potential threats and vulnerabilities, as well as to implement changes and monitor their results.[2] Such analyses should be conducted periodically and repeated as significant system changes occur. When security risks are identified, appropriate measures must be taken to reduce them. The result of risk analysis may point out security infrastructure holes (e.g., threats, vulnerabilities, and associated risks) that can be addressed through policy, training, and sometimes through new technology. Not all threats or vulnerabilities identified need to be addressed, but it is wise practice to document their assessment. An organization may elect not to address risks that have negligible impact. However, the resulting policies and procedures should be designed to prevent, detect, contain, and correct any security violations. These security risk analyses can be performed internally or by hiring outside professionals; nevertheless, direct involvement of the pathology laboratory leadership is advised.

In a recent guide to privacy and security of health information in the USA, the Office of the National Coordinator (ONC) for Health Information Technology (HIT) suggested five steps that are necessary to perform a security risk analysis [Figure 1]:[4,5]

1. Review current health information security.
2. Identify any threats and vulnerabilities.
3. Asses risks for likelihood and impact.
4. Mitigate security risks.
5. Monitor results.

During a security risk analysis process, all electronic systems or devices that play a role in generating, capturing, storing, or modifying patient data require

Table 1: Glossary of basic terms related to information security[a]

Glossary	
Adware	Software that automatically renders advertisements in order to generate revenue for its author
Anonymization	Process that removes or replaces identity information from a communication or record
Antivirus	Software used to prevent, detect, and remove malware
Audit	Evaluation process of a person, organization, system, process, enterprise, project or product
Authentication	Process of verification or confirmation of a user's identity
Backup	Process of copying and archiving computer data that can be used to restore the original after a data loss event
Bandwidth	Amount of data that can be transmitted in a fixed amount of time, usually expressed in bits per second (bps)
Biometrics	Unique, measurable characteristics of a human being that allow automatic recognition or identity verification
Certificate (key)	Data construct or alphanumeric string that serves as the basis for establishing a secure connection over the internet or a local network
Cloud computing	Use of computing resources (hardware and software) that are delivered as a service over a network (Internet)
Computer virus	Parasitic computer program that can replicate by infecting other computer files and spread from one computer to another; it almost always modifies and corrupts files on the targeted computers
Computer worm	Stand-alone computer program that replicates itself in order to spread to other computers, usually using computer networks, and has a direct effect on band-width
Confidentiality	Protection from unauthorized disclosure
Contingency plan	Plan designed for an outcome other than the usual (expected) plan
Covered entity	Group or organization that creates, transmits, receives, and maintains electronic protected health information (e.g., health-care plans, health-care billing companies, health-care providers)
Data integrity	Maintenance and assurance for the accuracy and consistency of data over its entire life-cycle
Data recovery	Process of salvaging data from damaged, failed, corrupted, or inaccessible storage media when it cannot be normally accessed
De-identification	Process by which a collection of data is stripped of information, that could allow identification of data source
Denial-of-service	Attempt to make a machine or network resource unavailable to its intended users
Disaster recovery	Process, policies, and procedures that are related to preparation for recovery or continuation of technology infrastructure after a disaster
Domain integrity	Pools of values from which actual values appearing in the columns of a table are drawn
Downtime	A period of time when a system is unavailable or when a system fails to provide or perform its primary function
Encryption	Process of changing readable text into a set of characters and numbers based on mathematical algorithms
Endpoint security	Methodologies and software that prevent workstations and other data access terminals from becoming unintended sources for unauthorized extraction of data by individuals authorized for review-only access. This includes provisioning for solutions that prevent peripheral devices, such as USB drives, from becoming data vectors
Entity integrity	Data integrity rule, which states that every table must have a primary key and that the columns chosen as primary key should be unique and not null
Firewall	System that acts as a filter between networks, preventing outside access to private networks or limiting access to the outside from within the network
High availability	System design approach and associated service implementation that ensures that a pre-arranged level of operational performance will be met
Malware	Malicious software used or created by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems (computer viruses, worms, trojan horses, spyware, adware, and other malicious programs)
Password aging	The process of forcing users to change access passwords with a specific frequency (password expiration)
Phishing	Attempt to acquire information such as usernames, passwords, or social security numbers by masquerading as a trustworthy entity in e-mails or text messages
Privacy	Protection from unauthorized intrusion
Referential integrity	Data integrity rule which states that any foreign-key value can only be in one of two states: a value that refers to another table's primary key value in the database, or a null value (no, or unknown relationship)
Role based access control (RBAC)	The process of restricting system access to authorized users based on their role

(Contd...)

Table 1: Contd...

Glossary	
Secure sockets layer (SSL)	Cryptographic protocol that provides communication security over the Internet
Security token	Physical device that an authorized user is using to ease authentication
Spyware	Malicious software installed on computers that collects information about users without their knowledge
Trojan horse	Malicious application that masquerades as a legitimate file or helpful program but whose real purpose is to grant the attacker unauthorized access to a computer
Two-factor authentication	Approach to authentication, which requires presentation of two authentication methods

[a]HIMSS. Terms and Acronyms, In: HIMSS Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations. ed. 2nd: HIMSS; 2010. *p* 1-130

Table 2: Topics discussed organized in relation to potential threats

Review section	Disasters	Security breaches	Privacy/ research
Security policies and procedures	X	X	X
Confidentiality		X	X
Data integrity	X	X	
Data availability	X	X	
Security risk analysis	X	X	X
System availability	X	X	
Disaster resiliency	X	X	X
Hardware security	X	X	
Endpoint security		X	
Software security		X	X
Passwords		X	X
Single sign-on		X	X
Biometrics		X	X
Access control		X	X
Audit trails		X	X
Data security measures			
Data integrity	X	X	X
Data protection strategies	X	X	X
Data recovery	X	X	X
Data encryption		X	X
Internet security			
Firewalls		X	X
Antivirus software		X	X
Interfaced instruments	X	X	X
Mobile devices	X	X	X
US regulations for health information security	X	X	X
Research data	X	X	X
Emergency situations	X	X	
Documentation	X	X	X

review. This includes LIS hardware and software as well as devices that can access LIS data (i.e., mobile devices such as tablet computers or smartphones) or interfaced devices such as instruments or point of care testing devices. Similarly, copiers and fax machines that can store data should be part of the review process.[6]

Organizations should establish audit programs to ensure that access to health information systems is appropriate and has not been compromised. As a rule, most organizations should complete full audit processes on an annual basis. Written policies are required to cover the mechanisms available to provide individuals with access to information systems. Policies and procedures for terminating access, such as when staff leaves the health-care organization need to be implemented. In addition, security awareness training should be provided to all staff members. Initial general training should be reinforced through periodic security reminders.

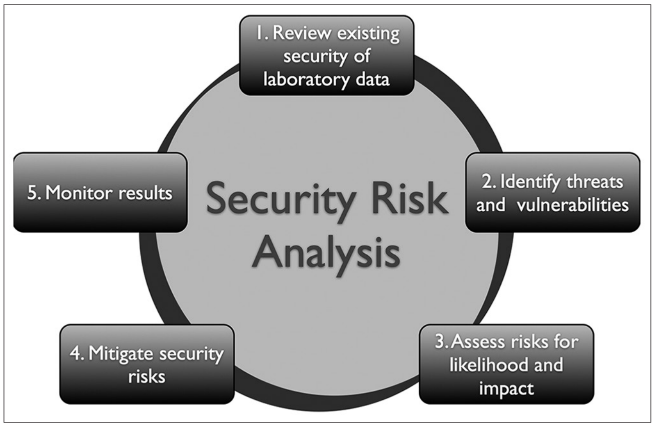
1. Review existing security of laboratory data
2. Identify threats and vulnerabilities
3. Assess risks for likelihood and impact
4. Mitigate security risks
5. Monitor results
Security Risk Analysis

Figure 1: Five steps of a security risk analysis process

SYSTEM AVAILABILITY AND DISASTER RESILIENCY

According to a study performed by Valenstein, *et al*., computers system down-time in the pathology laboratory varies widely between institutions and may occasionally be associated with adverse clinical outcomes.[7] Therefore, a major requirement of laboratory computer systems used to manage patient information is their reliability.[8] Laboratories (as well as health institutions in general) should have procedures for both planned and unplanned system outages (i.e., down-time procedures). For both types of outage, these procedures should address how the laboratory should function during the outage and the sequence and process by which all impacted software in the laboratory (LIS, middleware, instrument software, etc.) are brought back online once the outage has been resolved. For planned outages (i.e., down-time that occurs to perform system maintenance or an upgrade), the procedure should define the sequence as well as the process for shutting systems down. For unplanned events, procedures should assign responsibility for determination of the cause of the outage to defined individuals as well as the process and persons responsible for performing disaster recovery. Unplanned events can be classified into two broad categories: (i) natural disasters (e.g., floods, hurricanes, tornadoes or earthquakes), and (ii) man-made disasters. Disasters related to human error can include intentional destruction, technology conflicts, infrastructural failures, and accidents (such as a motor vehicle crashing into one's data center). While preventing some types of disaster may be difficult or impossible, setting up one's IT infrastructure to account for such a possibility can help reduce or avoid losses.[9,10]

Down-time procedures can use information garnered from a security risk analysis to help outline how an organization should react to any kind of outage. These should specify the laboratory's response based on the type of system outage (e.g., electronic health/medical record, LIS, instrument, network, phone system, paging system) and should be updated at least annually, or as systems and risks change. Down-time procedures also need to take into account both the infrastructure and personnel needs for the success of critical business operations during the outage. In addition, software support personnel should have defined procedures in place for checking the integrity of the data housed in systems and software once they are brought back online and before end-users' access is allowed back into the system.

Unplanned outages require additional steps for recovery, mainly the identification and resolution of the cause of the outage. Software support personnel should have troubleshooting procedures available for such events. In addition, an analysis of the effectiveness of the procedures should be performed after the down-time is resolved to determine if changes to these procedures would help improve efficiency and/or patient safety. Implementation of any measure that could prevent future occurrences of such outage should be performed.

Because any unplanned outage can result in data loss, it is critically important for the laboratory to develop robust data protection mechanisms that minimize loss and help speed the recovery process. Common strategies for data protection to consider include:

- Type of backup (periodic vs. real-time)
  - For periodic backups
    - Scope of backup (full vs. incremental)
    - Frequency of backup
  - For real-time backups
    - Switchover capability (business continuous/high availability; more labor intensive but cheaper)
- Location of backups (on-site, off-site or both)
- Backup media
  - Magnetic tape is cheap but is very slow
  - Storage area network technology which overcomes the need to restore data (only the systems will need to be restored or synchronized)
- Personnel to perform disaster recovery (internal vs. outsourced to a 3rd party).[11-13]

HARDWARE SECURITY

These safeguards relate to protection of the actual physical systems used to manage and store patient data.[14] Physical access (facility access control) to an area where servers, terminals, and modems are stored must be controlled (e.g., access cards), and the area should be locked at all times. Only authorized individuals should have physical access to hospital servers, and a log with all employees who have entered this area should be maintained. Physical safety of computer servers is achieved by using appropriate computer room facilities not only with security access, but also with controlled humidity, temperature, and fire protection. In case of fire in the computer room, water-based fire extinguishers should not be used because they may damage delicate electronic equipment. Carbondioxide (CO_2) is a safer fire extinguisher agent because it displaces oxygen and cools the reaction without being conductive or leaving toxic or corrosive residues.[15] Older computer rooms may contain Halon extinguishers. While this gas does not damage electronics, it is a chlorofluorocarbon gas and is no longer being deployed because, like Freon, it can damage the ozone layer. Newer agents that replaced Halon, with a similar mode of action, that act by removing the heat from the fire and not damaging the Ozone layer, are clean halocarbon agents (including FM-200, FE-25 and FE-13), and inert gases (which suppress fire by lowering oxygen concentration below the combustion level). All these agents are currently approved by the National Fire Protection Association and have advantages and disadvantages. Clean agent halocarbons require decreased storage space and can extinguish fire much quicker than inert gases, while the later can be piped up for a longer distance to reach the data center, and may perform better in rooms that are not sealed. Very early smoke detection apparatus (VESDA) can be employed to help detect early smoke or combustion products.[16]

It is also important to ensure that computer facilities have a stable power supply to avoid surges (voltage spikes) and outages. Electrical power disruptions are common events in both natural and man-made disasters. A sudden loss of power can cause data loss or possible hardware damage. Uninterruptible power supply devices have battery backups to temporarily maintain power to computers in the event of a power outage. Modern datacenters and hospitals typically have large generators deployed as electrical backup, yet even these can fail, thus, co-locations facilities are typically placed on a unique electrical grid from the primary facility.

Protection of patient data should also include procedures for the safe destruction of data on devices when the data is no longer needed, or when those device need to be discarded. These include all storage devices (old diskettes, tapes, flash drives, etc.). Policies and procedures for inventory control purposes and detailed databases of the inventory and configurations of the existing hardware can help in identifying missing equipment or altered internal configurations.

Endpoint Security

Endpoint security, as a subtype of hardware security, represents a different aspect of this requirement, where the covered entity (CE) is expected to protect the end-user physical abstraction layer of their IT infrastructure from becoming an originating point for breaches to unauthorized storage devices and portable computers. While there has been a consistent refinement of end point security approaches in the past decade for other IT sectors, use of such solutions in health-care IT has lagged, as many institutions and enterprises have so far altogether omitted addressing the issue.[17]

Given that any IT appliance (and specifically, end-user workstations/laptops) may be viewed as a conduit for en-masse extraction of data to other temporarily attached peripheral storage devices (e.g., Universal Serial Bus (USB) thumb drives and external Serial Advanced Technology Attachment (eSATA) disk drives), it is imperative that software/hardware solutions be adopted to thwart such connectivity, unless specifically authorized. With such solutions in place, for example, a USB thumb drive could no longer be used to allow for the unauthorized copying of one or more patient results records.

At present, many health-care institutions circumvent this sector of oversight by establishing local policy, making it a professional expectation that employees with access to systems containing ePHI will not attempt to generate unauthorized copies of such data on their own storage devices. However, in the long-term, it will become increasingly likely that central IT groups will be required to incorporate formal end point security solutions into their overall Physical Safeguard portfolio.

SOFTWARE SECURITY

Organizations should implement identity confirmation procedures for individuals or entities requesting access to ePHI. Each user that has access granted to the ePHI containing application must be assigned with a unique username that is never re-used, even if the original person to whom the username belonged has left the organization. The health-care institution should prohibit sharing of login information. A generic login may be used to log into a computer work-station, however, before using any information system application, users are required to authenticate. Authentication is the process of verifying or confirming the identity of a user that is requesting access to information. In the United States, the National Institute of Standards and Technology (NIST) issued an electronic authentication guideline that recommends four levels of assurance for authentication processes involved in electronic transactions.[18] To help with this process, especially in organizations where users have to access multiple information systems, various authentication tools are currently available including username-password pairs, single sign-on, biometrics (ID using human traits such as voice or fingerprints), and hardware or software tokens.[18] These mechanisms can also be used to authenticate the identity of users who are involved in the transport of specimens, slides, or other materials between multiple locations.[19]

Passwords

Passwords are currently the main mechanism used for user authentication. Therefore, proper enforcement of password use is critical. Organizations should use procedures for creating, changing, and safeguarding passwords. Covered entities need to enforce strong passwords for log on to information systems and medical applications.[20] The International Standards Organization (ISO), and other groups have recommendations for passwords.[21] In general, good passwords contain at least six characters (mixed lower- and upper-case) as well as numbers, and possibly even punctuation marks. Demanding users to select sophisticated passwords however, may result in passwords being written down.[22] Alternatively, password management tools can allow users to encrypt (by using a master password), organize, and save passwords on external media (i.e., USB flash-drive). Security questions may also be implemented to permit users easy recovery of forgotten passwords, bypassing additional calls to the computer services help-desk. Although current "best practices" suggest changing passwords every 90 days (password aging), this is controversial, especially in the health-care environment. A better approach could be a balance between strong passwords and longer time between required changes (e.g., 12 months). Password aging could possibly identify users who do not login to systems for an extended period of time. It is also recommended that only one login per user at a time should be allowed, and only one login session at a time. This permits ID and monitoring for password sharing and user's accounts should be locked after a maximum number of login attempts. Failed login attempts allow identification of unauthorized use of passwords.

Automated logout policies can be implemented so that after a certain period of inactivity the session is automatically disconnected from the system. However, if the automated logout time is too short it can interfere with systems usability.

A recent trend supporting increased password robustness is the use of so-called two-factor authentication, where a second credential is required in addition to the standard sign-on password. In one model, a key fob with a rotating pseudo-random multi-digit numerical key is used to provide the second factor (i.e., RSA Security Solutions, Inc.). Alternatively, a numerical key can be texted to the user's smart phone (i.e., Google Gmail, etc.). With this added layer in place, it becomes increasingly difficult to simply use a stolen username/password list to gain unauthorized access to HIPAA-covered systems.[23]

Single Sign-On

Single sign-on enables users to use one ID and password pair to access multiple related, but independent systems. The most common technique used is called Clinical Context Object Workgroup (CCOW). This is a standard written and adopted by Health Level Seven (HL7). It is vendor independent and allows users to obtain information about a specific patient from all interconnected systems. However, this does not allow the viewer to see any information belonging to another patient from any secondary systems. CCOW works for both client-server and web-based applications. Apart from the benefits of reducing password fatigue, single sign-on also reduces IT costs due to the decreased volume of password related help-desk calls. However, there are risks with single sign-on such as gaining access to multiple systems when one user name and password has been compromised. On a technical level, CCOW solutions should be implemented with significant care and diligence, as there have been a number of documented instances where CCOW synchronization errors have caused patient harm, owing to intermittent failure of the layer to keep all disparate applications pointed to the same patient instance. Thus, extensive local validation is needed prior to certifying any CCOW solution as being ready for clinical use.[24]

Biometrics

Biometric devices permit the use of Biometrics, which are unique and measurable characteristics of a human being that allow automatic recognition or identity verification.[25] Examples include fingerprinting, palm vein patterns, iris or retinal patterns recognition, speech scans and even sometimes DNA.[26] Although, DNA is still not a practical authentication method due to expense, time and intrusiveness involved, the iris pattern recognition is increasingly accepted and practical.[27,28] Biometrics are unique and their use makes it very difficult, if not impossible, to forge identity. However, biometric devices are not infallible; once a biometric file is intercepted, the patient's biometric could be definitively compromised. Thus, it is important that biometric data not be used for purposes the enrolled individual did not provide consent. In addition, the biometric template needs biometric authentication protection. This led to the development of Cancelable Biometrics and Biometrics Cryptosystems which, as an additional security measure don't have stored the full biometric template.[29] Employing more than one method of authentication, such as a password and fingerprinting, makes it more difficult for users to share credentials, thereby reducing the risks for unauthorized access.

Access Control

Information systems should have the ability to control, which users can have access to it and what information those users can view. In a Role Based Access Control (RBAC) system the access is granted based on user's roles (e.g., administrator, pathologist, resident, histotechnologist, etc.), and on the permitted role for specific information access (e.g., only read data, or provided with access to write, change, or delete data).[30] The RBAC system however, does have limitations. These often occur in the case of users that need different levels of access to perform their job. For example, a lab technician who works in hematology during the week, but on occasion covers the blood bank on weekends will need different levels of access to the clinical pathology LIS and blood bank systems. Similarly, some pathologists may be members of the quality improvement committee thus needing access to sensitive quality related data in addition to information required to perform their daily clinical work. Therefore, computer systems need capabilities to accommodate these special situations. Moreover, computer systems should have capabilities to override standard settings in the case of an emergency. Generation and maintenance of the RBAC list is a difficult task, requiring collaboration between information security personnel, human resources, clinical administration, and others. A data protection officer could oversee these activities. Maintenance activities include tracking when a user has changed roles or left the institution, or when the user's role itself needs to be modified.

Audit Trails

Modern LISs have capabilities to perform additional (random or by request) audits on access, record viewing, and modification of patient data. Written documentation of such reviews of information system activity (e.g., audit logs, access reports, security incident tracking reports) should be required so that they will be available during inspections or if questions arise about safety of data.[31]

DATA SECURITY MEASURES

Apart from the aforementioned security measures, there are many other factors that need to be considered when dealing with data in the pathology laboratory. This includes data integrity, protection, recovery, and encryption.

Data Integrity

Data integrity refers to the process of maintaining and assuring the accuracy and consistency of data over its entire life-cycle.[32] Therefore, data that has integrity is identically maintained during any operation, such as transfer, storage or retrieval (including back-up). In order to achieve this, certain rules need to be consistently and routinely applied to all data entering the system. Data integrity often includes checks and corrections for invalid data, based on a pre-defined set of rules. Data integrity is normally enforced in a database system by a series of integrity constraints rules, such as entity integrity, referential integrity or domain integrity [Table 1]. Out-dated and legacy systems that use file systems (i.e., text, spreadsheets, flat files, etc.) lack any kind of data integrity model. In the pathology laboratory it is important to verify the integrity of LIS after restoration of data files. This can be accomplished by reviewing a representative set of LIS-generated patient reports or by creating test ("dummy") patient reports for review.[33]

Data Protection Strategies

The pathology laboratory must be able to easily retrieve a complete copy of stored patient results, which includes all the pertinent associated data (e.g., original reference range used, annotations, etc.).[34] To protect electronic patient data, various methods and strategies can be enforced. Continuous data protection (CDP), also called continuous backup, refers to backup of data by saving it automatically every time the data is changed. This allows restoration of data (either file system or user data) to any point in time. Specialized software can provide fine granularity, allowing just the restoration of a particular file or type of files (e.g., mail boxes, database logs, etc.). While traditional backup can only restore data to the point at which the backup was taken (based on backup schedules), the continuous data approach allows for data restoration at any given time. This can be achieved by writing data not only to the original location on a disk, but also to a secondary location, usually another computer over a network.[12] Another advantage of CDP is that decreased backup media space is needed compared to the traditional backup. Usually, CDP saves byte or block-level differences rather than the entire modified file, while traditional backups make copies of entire files. However, a major disadvantage is the continuous bandwidth usage required with CDP. This may adversely affect network performance, especially for operations where file sizes are large. Throttling techniques that prioritize network traffic in order to reduce the impact of backup on day-to-day operations can be employed. Data can be divided and replicated among multiple physical drives using redundant array of independent disks (RAID, originally known as redundant array of inexpensive disks) storage technology. RAID allows data to be stored redundantly in a balanced way, to improve overall storage performance. A number of RAID levels were developed to provide different balance between performance, capacity, and tolerance, based on system's needs; however, currently there is no standard and RAID implementations can be proprietary and unique to individual vendors. RAID can be implemented as software (software manages mirroring of data that is stored on internal or external drives), controllers (hardware devices that have processing power that can be added to a server to offload the overhead of RAID from the CPUs), or storage arrays (multiple high-performance, redundant RAID controllers connected to multiple storage disks).[35] The use of RAID, as well as replication and mirroring, might protect only the most recent copy of data. When data corruption is not immediately detected, these technologies could actually protect corrupted data. Therefore, CDP technology allows data restoration to previous uncorrupted versions. Transactions that took place after the corrupting event will be lost in this setting; however, they could be recovered in other manner. Transaction logging is a process that records a history of all data modifications performed in a database, that guarantees reliability for hardware failure recoveries, and ACID (Atomicity, Consistency, Isolation, Durability) properties of database transactions. Database updates are saved in files located on a stable storage, and are used during a recovery process, permitting a complete data recovery.

Data Recovery

It is important for a laboratory to have procedures in place for their timely recovery from a destructive event. Data recovery implies salvaging data when it cannot be accessed normally due to damaged, corrupted or inaccessible secondary storage media (mass storage devices) related to the actual physical damage of the storage device, or to logical damage of the file system that prevents it from being mounted by the host operating system (OS).[13] Secondary media can be internal or external hard disk drives, solid state drives, USB flash drives, storage magnetic tapes, CDs, DVDs, or RAID. The most common scenario for data recovery is related to an OS failure. This can be accomplished by simply copying all the wanted files to a new disk from the backup media. The best approach is to have the disk partitioned, and to store valuable data files on a different partition than the replaceable OS system.

Another scenario involves files deleted from a storage medium. Usually, references to the deleted files in the OS directory structure are removed and the space they occupy is made available for later overwriting, but the contents of the deleted files may still be stored on the disk drive in a number of disconnected fragments, and may thus be recoverable. This type of data recovery can be achieved with specialized software. Such data recovery can be used in forensic applications, where data may not necessary be damaged, however, is hidden or encrypted. Solutions such as system snapshots or "ghost" copies of entire work-station are good strategies to backup and restore entire systems including, operating systems and installed application, which can allow for more rapid total system recovery.

Data Encryption

In the United States, HIPAA requires Covered Entities to notify individuals, if health related personal identifiable information is lost or stolen. However, this can be avoided if the lost personal identifiable information has been properly encrypted according to standards imposed by NIST.[33] Encryption disguises data, based on the mathematical algorithms, preventing it from being read, except by the intended recipient (who has the key). The original information is enciphered to become unreadable for unauthorized parties. An authorized party, on the other hand, can decrypt the data using a decryption algorithm (i.e., key). Applications are available for IT managers that can enforce the encryption of an entire hard drive of a computer or device (i.e., smartphone or tablet). Systems such as virtual private network technology leverage encryption to allow for secure communication over public networks by encrypting all data effectively and by creating a secure tunnel.

INTERNET SECURITY

The Internet enhances information and communication among individual work-stations and on a large scale between medical information systems. However, the Internet is a public environment with high-risk security threats. When LISs, instruments, workstations and/or mobile devices are connected to the Internet significant protection is required.[36] Personal computer (PC) security in the era of Internet connectivity involves not only safeguarding computers and networks themselves, but also protecting the information that is stored and transmitted. Laboratory computers may be exposed to many security risks (e.g., intrusion from hackers, viruses from emails, spyware, denial-of-service attack, phishing, and so on). All laboratory personnel including pathologists should have a basic understanding of Internet security threats and should be in compliance with their organization's policies and procedures to avert them. There is always a tradeoff between the level of protection desired and the cost of protection enforcement or systems functionality.[37] Internet security involves both network and browser security measures. Network layer security often uses protocols such as Secure Sockets Layer (SSL) for web traffic. A SSL connection allows the browser and server of a web transmission to authenticate identities and encrypt data transferred. SSL works by using a private key to encrypt data that is being transferred. In so doing, SSL ensures that data that came from a web server is in the original form, and that no one tampered with it. Web servers that support SSL sessions have web addresses that start with "https" instead of "http." In the United Stated, HIPAA requires that all Internet transmissions containing patient data are sent using at minimum SSL to protect confidentiality.[38,39]

Firewalls

Firewalls are systems that act as filters between networks preventing outside access to private networks, or limiting access to the outside from within the network. They can be hardware, software or a combination of both. Software can analyze incoming or outgoing data to determine whether they are appropriate and if they meet criteria to be granted access to the network. Firewalls can limit systems functionality; for example, they may sometimes block signals required to remotely control robotic microscopes during telepathology. Firewalls are maintained by system administrators, who are responsible for the implementation of organization's policies on network access.[40,41]

Antivirus Software

There are many different kinds of malware (malicious software). Protection from malicious software is critical due to the increased number and severity of cyber-attack threats. Software viruses are computer programs that can replicate themselves and spread from one computer to another; they are written intentionally to alter a computer's operation and almost always corrupt or modify files on targeted computers. Trojan horses are malicious applications masquerading as legitimate software that can grant hackers unauthorized access to computers. They don't replicate in computer files, however, when installed usually in tandem with other applications downloaded online, can allow hackers to harm host computers or to steal locally stored information. Spyware are software applications designed to monitor users' computing; they can collect almost any type of data, including login passwords. Computer worms are stand-alone malware applications that replicate to spread to other computers, usually, through computer networks. Even if there is no direct harm to computer files, they can slow-down network data transmission by consuming bandwidth.[42] Antivirus software can detect and protect computers and networks from malware, however to be effective they need to be properly used. They have to be correctly configured for automated, regular virus definition updates and file scanning. Internet security software suites provide additional safety, typically, adding firewalls and application access control or privacy features. Workforce education and implementation of policies and procedures that prevent malicious software installation, although, not currently required by law, are highly recommended.

INTERFACED INSTRUMENTS

Interfaced instruments have unique security challenges and requirements. Whereas, in the past most instruments controllers used proprietary operating systems and dedicated network communication protocols, these days they use widely windows based operating systems and Transmission Control Protocol and Internet Protocol (TCP/IP) based network protocols for communications. This exposes laboratory instrumentation to the same type of security issues discussed for PC's, servers, and mobile devices. Therefore, instrument's OS and hardware protection must be approached similarly to typical computers. Further, vendors typically will request appropriate secure Internet-based access to these devices by using technology such as virtual private networks (VPN). This allows for significant improvement in support and troubleshooting, that must be supported. These requirements are mandated by a specific Clinical and Laboratory Standards Institute (CLSI) standard.[38] As a result, placing an instrument with an OS (Windows), requires planning for monitoring access, setting up secure vendor access, installation of antivirus software, and planning for backup and restoration in case of system failure. One complexity often encountered is that these "medical devices" may not come under the jurisdiction of the larger IT group, but rather the medical device support group. The fact that computers associated with these instruments were placed by an outside vendor can create controversy over the installation of antivirus software or the use of institutional backup and restore software due to perceived or actual license restrictions. Furthermore, given these devices complexity, antivirus software could potentially interfere with the required communications, as could both firewalls and proxy servers.

MOBILE DEVICES

The increased use of mobile devices (e.g., smartphones, tablet computers) and wireless medical devices (e.g., point-of-care-testing) in health-care realm pose serious challenges for organizations, with respect to ensuring data security and integrity.[43-45] Clinicians are increasingly demanding to have laboratory results and critical values communicated directly to their mobile devices. To protect ePHI, institutions that permit the use of mobile devices need to develop new policies for their appropriate clinical use, and to adopt cost-effective ways to manage their security. However, currently there are limited standards with respect to the use of wireless data in health-care.[39,41,46] In 2005, the Food and Drug Administration issued a notice entitled "Cyber-security for Networked Medical Devices is a Shared Responsibility".[47] Nevertheless, new regulations related to secure authentication for mobile devices,[48] options to track and secure mobile devices remotely by locking or wiping out information,[49] or for the use of clinical software on personal mobile devices are still needed. New policies (e.g., use of secure text messages and secure e-mail communication) and technologies (e.g., cloud computing that can allow physicians to send and receive encrypted messages on mobile devices) are currently being developed to overcome some of these security issues.[50] Pathology informaticists should be prepared to handle data from the next generation of health-care technologies, such as in-home patient monitoring devices, that could push lab-related data directly to the hospital's electronic medical record.[51]

US REGULATIONS FOR HEALTH INFORMATION SECURITY

Under HIPAA, pathology laboratories are legally required to securely acquire, analyze, store, and transmit the vast amounts of electronic data they handle. According to HIPAA, health information that is associated to an identifiable patient is known as Individually Identifiable Health Information (IIHI). A subset of this type of information is known as Protected Health Information (PHI). The legal definitions of these terms are presented in Table 3.[52] Laboratory results in combination with unique patient demographics and patient identifiers constitute PHI, regardless of form. Because laboratory accession numbers are designed to uniquely identify a patient within a health facility, these also should be treated as PHI according to the last item in the list of identifiers from the 45 CFR (Code of Federal Regulations) Sect 164.514, "any other uniquely identifying code, characteristic or number" [Table 4].[52] If one fails to remove an accession number from a specimen during de-identification, the burden will be on that individual to demonstrate why an accession number could not be used alone or in combination with other information to identify an individual. If it is very easy to remove the specimen number, the legal system could be less inclined to accept the documented risk analysis by weighting any risks relative to the efforts required to remove that information.

In the United States, HIPAA governs privacy and protection of medical information and health records.[53] The initial HIPAA rules, enacted by the federal government in 1996, were related to the administration of health insurance and aimed at improvement of continuity and availability of health insurance coverage, as well as at the prevention of waste, fraud, and abuse

Table 3: Legal definitions related to health information

Term	Definition
Individually identifiable health information (IIHI)	Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual
Protected health information (PHI)	Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer
Electronic protected health information (ePHI)	Information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information

Table 4: Legal requirements for de-identifying protected health information

45 CFR Sect 164.514 (b)(2)

(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

(D) Telephone numbers

(E) Fax numbers

(F) Electronic mail addresses

(G) Social security numbers

(H) Medical record numbers

(I) Health plan beneficiary numbers

(J) Account numbers

(K) Certificate/license numbers

(L) Vehicle identifiers and serial numbers, including license plate numbers

(M) Device identifiers and serial numbers

(N) Web Universal Resource Locators (URLs)

(O) Internet Protocol (IP) address numbers

(P) Biometric identifiers, including finger and voice prints

(Q) Full face photographic images and any comparable images

(R) Any other unique identifying number, characteristic, or code; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information

in the health-care industry. According to this act, an individual's PHI has to be kept confidential and only used in his/her best interests.[54] Only personnel involved in a particular patient's care are considered to have a business relationship (with this often referred to as a "need-to-know" basis), and therefore, are authorized to access that patient's medical record. Three components related to the privacy and security of PHI, were initially included in this act: creation of a federally managed system of unique patient identifier, safeguards to protect that identifier and transaction formats for health information. These were also considered building blocks for the creation of the National Health Information Network (NHIN).[55] Unfortunately, 2 years later congress repealed the health identifier (which would have been a major advance for the US medical care systems), yet left in place the draconian security measures designed only to protect that identifier. HIPAA also required privacy regulation to be issued by the United States Department of Health and Human Services (HHS).

The final version of this privacy regulation, known as the HIPAA Privacy Rule, was issued on December 28, 2000.[56] This Rule gives patients certain rights over their health information, including the right to obtain and examine a copy of their health record and to request an amendment of their record. At the same time, it requires safeguards to protect the privacy of PHI.[56] Covered Entities have the right to decline a patient's request but must document the reasons for declining to release the data requested.[57] The Privacy Rule encouraged the development of health information systems by establishing standards and requirements for the electronic transmission of certain health information. Modifications to the Privacy Rule were issued in August of 2002, which established national standards for protection of health information, including unique health identifiers for individuals, employers, health plans, and health-care providers, as well as electronic transmission, and authentication of signatures.[52]

Per HIPAA, a CE is any group or organization that creates, transmits, receives, and maintains PHI, including ePHI. These encompass health-care plans, health-care billing companies, or health-care providers. A Business Associate (BA) is a person or organization, other than a member of a CE's workforce, that performs certain functions or activities on behalf of, or provides certain services to a CE, that involve the use or disclosure of individually identifiable health information. HIPAA applies to all Covered Entities and to BAs.[58]

Concurrently with the development of the privacy rule, the secretary of HHS was required to publish national standards for the security of ePHI under the administrative simplification provisions of HIPAA, presumably due to the continuous growth of electronic data use and proven cases of ePHI misuse. The proposed rule for electronic security of ePHI was issued for comment on August 12, 1998 but was not finalized until almost 5 years later on February 20, 2003.[59] Known as the HIPAA Security Rule, it mandates appropriate administrative, physical, and technical safeguards to ensure confidentiality, integrity, and security of ePHI.[59] Hence, the Security Rule applies only to PHI in electronic form, while the Privacy Rule consists of security standards that apply to PHI in any medium. Faxes, if they originate on paper, are specifically excluded from the security rule. Both, the security rule and the privacy rule require CE to implement safeguards to protect PHI. However, the privacy rule provides no specific details and simply requires that CE reasonably protect PHI with appropriate safeguards, while the Security Rule specifies 43 categories of safeguards [Tables 5-7].[3,60] Each safeguard is listed as either required or addressable. Required safeguards must be implemented. Covered entities must evaluate addressable safeguards for feasibility and appropriateness. If the safeguard is not implemented, the CE must document the reasons for that decision. When it is decided that the addressable specifications are not appropriate, documentation, including alternative methods, is imperative. Health-care organizations can go above and beyond the law by implementing greater data protection measures than what it is required by law (with the caveat that implementing such expanded measures imparts a regulatory expectation that they will be assiduously followed). These requirements can have significant impact on the computing within an organization, limiting workflow and creating barriers to adoption of valuable information technology. HIPPA regulations also require that covered entities have notice of privacy practices posted online on the public domain, available for patient access, and similar notices distributed with inpatient/outpatient registration questionnaires given to patients.[61]

The Health Information Technology for Economic and Clinical Health Act (HITECH), signed into law in the USA on February 17, 2009, modified a number of HIPAA regulations.[62] Both CE and BA are required to report breaches of security, while the penalties for unauthorized disclosure are stiffened.[62,63] The Security Breach Notification Rule within HITECH requires CEs and their BAs to notify any affected patient when the security of their PHI has been compromised according to predefined guidelines, in no case later than 60 days following the breach discovery. If there is insufficient contact information for 10 or more affected individuals, the CE must post the notice on the home page of its web site, or provide it in major print or broadcast regional media where the affected individuals likely reside. For security breaches that affect more than 500 identified individuals, CEs must notify the Secretary of HHS, as well as prominent media outlets, in addition to satisfying the previously mentioned notification of patients; breach of fully de-identified data is not considered as a reportable event. HHS maintains a public and searchable web site with records of these breaches.[64] Between September

Table 5: Administrative safeguards according to HIPAA (Security policies and procedures)

Standard	Required implementation	Addressable implementation
Security management functions	Risk analysis Risk management Sanction policy Information system activity review	
Assigned security responsibility	Identify responsible official	
Workforce security		Authorization and supervision Workforce clearance procedures Termination procedure
Information access management	Isolate clearinghouse functions	Access authorization Access establishment and modification
Security awareness and training	Periodic security reminders Protection from malicious software Log-in monitoring Password management	
Security incident procedure	Response and reposting	
Contingency plan	Data backup plan Disaster recovery plan Emergency mode operation plan	Testing and revision procedures Applications and data criticality analysis
Evaluation	Periodic technical and non-technical evaluations	
Business associated contracts and other arrangements	Written contracts	

Table 6: Physical safeguards according to HIPAA (Hardware security)

Standard	Required implementation	Addressable implementation
Facility access control		Contingency operations Facility security plan Access control and validation Maintenance records
Workstation use	Policies for appropriate use of workstations	
Workstation security	Restrict access to authorized users	
Device and media controls	Disposal Media reuse	Accountability Data backup and storage
Endpoint security		Peripheral storage device data containment plan En masse data breach countermeasure

Table 7: Technical safeguards according to HIPAA (Software Security)

Standard	Required implementation	Addressable implementation
Access control	Unique user identification Emergency access procedure	Automatic logoff Encryption & decryption
Audit control	Examine system use	
Integrity	Authenticate electronic protected health information	
Person or entity authentication	Authentication prior to granting access	
Transmission security		Integrity control Encryption

2009 and November 2012 there have been 511 security breaches of this type reported in the U.S, affecting over 21 million individuals in total. Most of the reported breaches involved ePHI including, loss, theft, hacking, and unauthorized access of laptops, backup tapes, computers, servers or portable electronic devices. Loss of large sets of patient data was primarily due to theft (52.18%) or accidental disclosure (18.39%). The location of data at the time of loss has been overwhelmingly on paper (25.29%) or on a laptop (25.06%).[65] Breaches affecting fewer than 500 individuals are required to be reported in a more limited fashion, to the HHS on an annual basis.

Encrypted data does not need to be reported. For example, in late 2012, a University of Michigan clinical investigator's laptop was stolen from a vehicle. Although, the PC contained tens of thousands of identified results, the laptop featured the standard enterprise-issued, full-disk, NIST-compliant encryption, thus, meeting the safe harbor provision under the HITECH act. Consequently, there was only the fiduciary need to carry out a breach analysis, locally, with no further need to file a data incident report with HHS.

With HITECH, penalties for unauthorized disclosures, including those associated with security breaches related to health information have been substantially increased.[62] Currently, for a single unauthorized disclosure, convicted individuals, CE or BA can be fined from $100 to up to $50,000, or face imprisonment, depending on the level of intent to do harm. During a single calendar year, the maximum fine for all unauthorized disclosures for a particular CE or BA is $1.5 million. A study performed by a major privacy and security research center in 2011 found that the frequency of reported data breaches among 72 organizations surveyed increased by 32% from the previous year, generating a significant increase (10-fold) in associated costs (i.e., fines, communication, remediation, loss of strategic partners or patients). Unsecured mobile devices were particularly responsible for these vulnerabilities.[66]

RESEARCH DATA

The use of human samples and related health-care data for research purposes has been invaluable in the past and will become critical in the near future, especially, with the implementation of genomics and proteomics. Development of grid-based systems such as the Cancer Biomedical Informatics Grid (caBIG), may better assist with these tasks; however, they pose new data security challenges to participating pathology laboratories, including new regulatory measures.[5] It is the ability to connect a unique individual with private medical information, that causes most of the concern for unauthorized disclosure. The legal requirements in the United States under which health information can be de-identified is presented in Table 4. Therefore, when dealing with biomedical informatics research, De-identification and Anonymization (e.g., data scrubbing using the doublet method)[67] are important techniques to minimize potential loss of patient confidentiality and privacy. Moreover, access and use of this type of data must be strictly enforced and restricted to the purpose defined in the informed consent. Disclosure results filters and query restrictions are two of the proposed methods to enforce data privacy in this context; the software interface removes data that is not supposed to be seen by the requester from the query results.[51] In the U.S., before pathology data can be used for research purposes, laboratory needs to make sure that its use complies with HIPAA, the Common Rule,[63,68-70] and with the Institutional Review Board (IRB) guidelines. As a general rule, patient data to be used for research studies should be fully de-identified, unless there is a compelling need for the use of identified or anonymized data sets (e.g., for longitudinal studies, where matching new results to prior results is paramount). Typically, it is the role of the IRB to determine the level of patient data identification that will be allowed for any given study. Finally, in settings where anonymized data is to be used, many institutions have adopted the concept of an "honest broker" clearing house that manages the codebook between fully identified data, as housed in the institution's primary repositories, and the anonymized data set, as used by individual investigators. In this manner, the research team has no possibility of accidentally discovering the identity of their study subjects. Most importantly, this investigative model has been thoroughly reviewed and approved by the federal government's Office for Human Research Protections, making the Honest Broker model an important operational element of any enterprise considering clinical research.[5,71]

EMERGENCY SITUATIONS

It is very important that an emergency service is available for all key hardware and software being used in the laboratory. In the U.S, HIPAA requires procedures for accessing necessary ePHI during emergency situations. IT managers may need to recover access to computers, even if they are protected with Basic Input/Output System (BIOS)-level security, full disk encryption, and strong, multi-factor authentication. The Security Rule mandates emergency access procedures.[59] They have to be activated in the case of a potential life-threatening situation, when a physician or other member of the health-care team needs immediate access to information to which they normally do not have access. These types of procedures are called "break-glass" access procedures. An emergency access solution should be utilized only when normal processes are insufficient (e.g., the help-desk or system administrators are unavailable).

DOCUMENTATION

Policies (rules to guide decisions), and procedures (usually process descriptions) that deal with IT security-related issues in the laboratory should be made available to users and IT staff in the laboratory. In order to comply with the HIPAA Privacy and Security Rules, covered entities are required to develop appropriate written policies and procedures for each standard implementation, and to periodically review and update them. Policies and procedures should document adherence to regulatory requirements as well as handling of staff violations. They need to be communicated to staff in an understandable way, and compliance has to be monitored on a regular basis, through audit and risk analysis processes. The laboratory director is responsible with the regular review of written policies and procedures, as well as of any written records of assessments, actions or activities, (e.g., at least annually or when a major system changes). In addition, it is important that division of pathology informatics documents any maintenance, modifications, customizations, testing after modifications, validation activities, down-time (scheduled or unscheduled), and user training they are involved with.

CONCLUSION

Given that pathology laboratories are heavily involved in dealing with patient information for clinical and possibly research purposes, policies, and procedures that deal with data protection and security are critical. Contemporary pathology laboratories need to address security concerns due to increased connectivity of their information systems and work-stations to the Internet, as well as to address the demand for wireless and mobile devices use. A fundamental activity for laboratories, at least in the USA, is to remain compliant with HIPAA and HITECH. The most recent updates made to the HIPAA Privacy and Security Rules were published in January 2013 and were effective beginning March 26, 2013. They implemented HITECH, strengthened privacy protections under Genetic Information Non-discrimination Act, and included other changes, especially, affecting BAs. According to these new updates, BAs became subject to direct civil penalties if found responsible for privacy or security breaches.[72]

Helpful resources that pathologists and laboratory personnel responsible for patient data privacy and security should have handy include:

- College of American Pathologists checklists for laboratory accreditation.[73] These checklists include a special section for laboratory computer services, which covers all major aspects of LISs and computer services in the laboratory, including privacy and security of patient data. In addition, special stipulations related to confidentiality and security of patient data for telepathology services, are addressed.
- Centers for Medicare and Medicaid Services published educational materials and guidelines related to compliance with HIPAA, privacy and security standards, and health insurance reform.[59]
- CLSI published technical and operational standards, as well as technical implementation procedures related to security of *in vitro* Diagnostic (IVD) systems (devices, analytical instruments, data management systems, etc.) installed at a health-care organization. The AUTO11-A-IT Security of IVD Instruments and Software Systems document is intended for vendors, users (e.g., laboratory personnel), and the IT management of health-care organizations.[74]
- The Information Security Task Force of the International Society of Blood Transfusion developed and published guidelines for information security in transfusion medicine. These guidelines address the applicability of the HIPAA Security Standards in Transfusion Medicine.[75]

In today's environment, LISs are almost never relied upon (besides true, core laboratory workers) for data retrieval or reference. Laboratory data is uploaded, many times to multiple Electronic Medical Records, and even when the LIS is the most secure environment, risks still exist for those data to be compromised because of systems that are not under the laboratory control. Therefore, it is essential to have a full and unwavering organization-wide commitment to the security of PHI.

REFERENCES

1. Ulirsch RC, Ashwood ER, Noce P. Security in the clinical laboratory. Guidelines for managing the information resource. Arch Pathol Lab Med 1990;114:89-93.
2. Hutfless B. Privacy and Security. In: Hoyt RE, Sutton M, Yoshihashi A, editors. Medical Informatics: Practical Guide for Healthcare and Information Technology Professionals. 4th ed: www.lulu.com; 2010. *P* 12-42
3. Golightly C, Tuthill JM. Laboratory information system operations. In: Pantanowitz L, Tuthill JM, Balis UGJ, editors. Pathology Informatics: Theory and Practice. Chicago: ASCP Press; 2012. p. 117-34.
4. The Office of the National Coordinator for Health Information Technology. Privacy and Security and Meaningful Use. In: Guide to Privacy and Security of Health Information. http://www.healthit.gov; 2012. p. 9. Available from: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. [Last cited on 2012 Nov 29].
5. Manion FJ, Robbins RJ, Weems WA, Crowley RS. Security and privacy requirements for a multi-institutional cancer research data grid: An interview-based study. BMC Med Inform Decis Mak 2009;9:31.
6. Ham NJ, Boothe JF. Can you keep a secret? Give your lab results a HIPAA privacy checkup. Med Lab Obs 2003;35:32-4.
7. Valenstein P, Treling CP, Aller RD. Laboratory computer availability: A college of American Pathologists Q-probes study of computer downtime in 422 institutions. Arch Pathol Lab Med 1996;120:626-32.
8. Valenstein P, Walsh M. Six-year trends in laboratory computer availability. Arch Pathol Lab Med 2003;127:157-61.
9. Abir M, Mostashari F, Atwal P, Lurie N. Electronic health records critical in the aftermath of disasters. Prehosp Disaster Med 2012;27:620-2.
10. David W. In disasters such as Sandy, HIE is 'as critical as having roads, as having fire hydrants'. Healthcare IT News; 2012. p. 1-5. Available from: http://www.healthcareitnews.com. [Last cited on 2012 Nov 29].
11. Post DC. Protecting your most valuable practice asset: Your data. Understanding the technology of Internet offsite data backup. Tex Dent J 2009;126:720-1.
12. Repasky L, Heard S. Preventing data disasters: Helpful tips on data backup and storage options. MGMA Conne×2010;10:46-9, 1.
13. Halpert AM. Complying with the privacy rule during a disaster–Part 1. An overview of plan development, data backup, and recovery. J AHIMA

2008;79:60-1.

14. Riha C. Protecting and securing networked medical devices. Biomed Instrum Technol 2004;38:392-6.
15. Park S, Balis UG, Pantanowitz L. Computer fundamentals. In: Pantanowitz L, Tuthill JM, Balis UG, editors. Pathology Informatics: Theory and Practice. Chicago: ASCP Press; 2012. p. 11-34.
16. Kroll K. Fighting Fires In Data Centers, 2007. http://www.facilitiesnet.com. Available from: http://www.facilitiesnet.com/datacenters/article/Fighting-Fires-in-Data-Centers--6657. [Last cited on 2012 Nov 29].
17. Acosta JC, Medrano JD. Using a novel blending method over multiple network connections for secure communication. MILCOM-2011. Military Communications Conference; 2011. p. 1460-5.
18. Burr WE, Dodson DF, Polk WT. Information security. In: Electronic Authentication Guideline. National Institute of Standards and Technology (NIST) Special Publication 800-63; 2011. p. 1-121. Available from: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. [Last cited on 2012 Nov 29].
19. Tomlinson JJ, Elliott-Smith W, Radosta T. Laboratory information management system chain of custody: Reliability and security. J Autom Methods Manag Chem 2006;2006:74907.
20. El Emam K, Moreau K, Jonker E. How strong are passwords used to protect personal health information in clinical trials? J Med Internet Res 2011;13:e18.
21. Sahibudin S, Sharifi M, Ayat M. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. Proceedings of the 2008 Second Asia International Conference on Modelling \ and Simulation (AMS). IEEE Computer Society; 2008. p. 749-53.
22. Cipresso P, Gaggioli A, Serino S, Cipresso S, Riva G. How to create memorizable and strong passwords. J Med Internet Res 2012;14:e10.
23. Hsiao TC, Liao YT, Huang JY, Chen TS, Horng GB. An authentication scheme to healthcare security under wireless sensor networks. J Med Syst 2012;36:3649-64.
24. Berger RG, Baba J. The realities of implementation of clinical context object workgroup (CCOW) standards for integration of vendor disparate clinical software in a large medical center. Int J Med Inform 2009;78:386-90.
25. Flores Zuniga AE, Win KT, Susilo W. Biometrics for electronic health records. J Med Syst 2010;34:975-83.
26. Thompson CA. Biometrics offers alternative to password entry. Am J Health Syst Pharm 2005;62:1115-6.
27. Smith AD. Biometrics-based service marketing issues: Exploring acceptability and risk factors of iris scans associated with registered travel programmes. Int J Electron Healthc 2008;4:43-66.
28. Leonard DC, Pons AP, Asfour SS. Realization of a universal patient identifier for electronic medical records through biometric technology. IEEE Trans Inf Technol Biomed 2009;13:494-500.
29. Teoh AB, Kuan YW, Lee S. Cancellable biometrics and annotations on BioHash. Pattern Recogn 2008;41:2034-44.
30. Wager KA, Lee FW, Glaser JP. Security of health care information systems. In: health care information systems: A Practical Approach for Health Care Management. San Francisco: Jossey-Bass; 2009. p. 251-78.
31. Coleman RM, Ralston MD, Szafran A, Beaulieu DM. Multidimensional analysis: A management tool for monitoring HIPAA compliance and departmental performance. J Digit Imaging 2004;17:196-204.
32. Smith A, Greenbaum D, Douglas SM, Long M, Gerstein M. Network security and data integrity in academia: An assessment and a proposal for large-scale archiving. Genome Biol 2005;6:119.
33. Schweitzer EJ. Reconciliation of the cloud computing model with US federal electronic health record regulations. J Am Med Inform Assoc 2012;19:161-5.
34. Korpman RA. System reliability. Assurance of quality and security. Clin Lab Med 1983;3:165-77.
35. Patterson DA, Gibson G, Katz RH. A case for redundant arrays of inexpensive disks (RAID). SIGMOD Rec 1988;17:109-16.
36. Liu CH, Chung YF, Chen TS, Wang SD. The enhancement of security in healthcare information systems. J Med Syst 2012;36:1673-88.
37. Caruso RD. Personal computer security: Part 1. Firewalls, antivirus software, and Internet security suites. Radiographics 2003;23:1329-37.
38. CLSI. Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Proposed Standard; www.clsi.org 2012. Available from: http://www.clsi.org.
39. Luxton DD, Kayl RA, Mishkind MC. mHealth data security: The need for HIPAA-compliant standardization. Telemed J E Health 2012;18:284-8.
40. Kwon J, Johnson ME. Security practices and regulatory compliance in the healthcare industry. J Am Med Inform Assoc 2013;20:44-51.
41. Yeo K, Lee K, Kim JM, Kim TH, Choi YH, Jeong WJ, *et al*. Pitfalls and security measures for the mobile EMR system in medical facilities. Healthc Inform Res 2012;18:125-35.
42. Cadick R. Protecting networked medical devices from worms and viruses. Biomed Instrum Technol 2004-2005;Suppl: 21-2.
43. Bergeron BP. Wireless local area network security. J Med Pract Manage 2004;20:138-42.
44. Pancoast PE, Patrick TB, Mitchell JA. Physician PDA use and the HIPAA Privacy Rule. J Am Med Inform Assoc 2003;10:611-2.
45. Pharow P, Blobel B. Mobile health requires mobile security: Challenges, solutions, and standardization. Stud Health Technol Inform 2008;136:697-702.
46. Croll PR, Ambrosoli KM. Privacy with emergency medical information used in first response. Stud Health Technol Inform 2012;178:7-13.
47. Murray JF. Guidance for industry: Cybersecurity for networked medical devices containing Off-The-Shelf (ots) software. Food and Drug Administration; 2005. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf. [Last cited on 2012 Dec].
48. Gao L, Dai H, Zhang TL, Chou KC. Remote data retrieval for bioinformatics applications: An agent migration approach. PLoS One 2011;6:e20949.
49. Kuppusamy KS. A Model for remote access and protection of smartphones using short message service. IJCSEIT 2012;2:95-104.
50. Prestigiacomo J. Secure messaging via the cloud and mobile devices: Data security issues emerge with new technologies. Healthc Inform 2011;28:24-9.
51. Meingast M, Roosta T, Sastry S. Security and privacy issues with health care information technology. Conf Proc IEEE Eng Med Biol Soc 2006;1:5453-8.
52. Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information; Final Rule. 45 CFR Parts 160 and 164. www.hhs.org; 2002. Vol. 45.
53. U. S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA). www.cms.org; 1996. Available from: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/hipaalaw.pdf. [Last cited on 2012 Nov 29].
54. Ham NJ, Booth JF. Lab results delivery in the context of HIPAA compliance. Med Lab Obs 2001;33:32-5.
55. Greenberg MD, Ridgely SM. Patient identifiers and the national health information network: Debunking a false front in the privacy wars. J. Health and Biomedical L 2008;4:31-68.
56. Department of Health and Human Services. Standards for privacy of individually identifiable health information. Office of the Assistant Secretary for Planning and Evaluation, DHHS. Final rule. Fed Regist 2000;65:82462-829.
57. Lebowitz PH. The HIPAA privacy rule: Clinical laboratories must comply. Am Clin Lab 2002;21:35-6.
58. Goedert J. Keeping an eye on business associates. Health Data Manag 2011;19:40-3.
59. Centers for Medicare and Medicaid Services (CSM), HHS. Health insurance reform: Security standards. Final rule. Fed Regist 2003;68:8334-81.
60. Sinard JH. External regulations pertinent to LIS management. In: Practical Pathology Informatics: Demystifying Informatics for the Practicing Anatomic Pathologist. New York: Springer Science and Business Media; 2006. p. 325-53
61. Kiel JM. HIPAA and its effect on informatics. Comput Inform Nurs 2012;30:1-5.
62. US Department of Health and Human Services. Health Information Technology for Economic and Clinical Health Act Enforcement Interim Final Rule. www.hhs.gov; 2009. Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf. [Last cited on 2012 Nov 29].
63. Rinehart-Thompson LA, Hjort BM, Cassidy BS. Redefining the health information management privacy and security role. Perspect Health Inf Manag 2009;6. Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2781727/. [Last cited on 2012 Nov 29].
64. Breaches Affecting 500 or More Individuals. Volume 2012: The Office of the National Coordinatory for Health Information Technology. www.hhs.gov; 2012. Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/

breachnotificationrule/breachtool.html. [Last cited on 2012 Nov 29].

65. Patel CD, Carter AB. The department of health and human services wall of shame: An analysis of large security breaches of protected health information. J Pathol Inform 2012;3:S45.
66. Raths D. Unsecured mobile devices: The weak link. Healthc Inform 2012;29:60-1.
67. Berman JJ. Text Scrubber for Deidentifying Confidential Text. In: Methods in Medical Informatics: Fundamental of Healthcare Programming in Perl, Python, and Ruby. Boca Raton, FL: Chapman & Hall/CRC; 2011. p. 219-25.
68. US Department of Health and Human Services. Protection of Human Subjects. Department of Health and Human Services; 2009. p. 45. Available from: http://www.hhs.gov/ohrp/policy/ohrpregulations.pdf. [Last cited on 2012 Nov 29].
69. US Department of Health and Human Services. Code of Federal Regulations Title 45 Public Welfare. Part 46 Protection of Human Subjects. Washington, D.C: Department of Health and Human Services; 2012. p. 1-14.
70. Grizzle WE, Woodruff KH, Trainer TD. The pathologist's role in the use of human tissues in research – Legal, ethical, and other issues. Arch Pathol Lab Med 1996;120:909-12.
71. Butler D. Biotech industry seeks 'honest brokers'. Nature 1999;398:360.
72. Services DoHaH. Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the health information technology for economic and clinical health act and the genetic information nondiscrimination act; other modifications to the HIPAA rules. Federal Register. Federal Register: Department of Health and Human Services; 2013. p. 5565-702. Available from: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. [Last cited on 2012 Jan 31].
73. Commission on Laboratory Accreditation. Laboratory General Checklist. Northfield, IL: College of American Pathologists; 2009. p. 1-100.
74. Knafel AJ, Chou D, Crocker B, Davis RR, Olson E, Wood DO, *et al*. IT security of *in vitro* diagnostic instruments and software systems; approved standard. CLSI document AUTO11-A. 2nd ed., Vol. 26. Wayne, PA: Clinical and Laboratory Standards Institute (CLSI); 2006. p. 1-43.
75. International Society of Blood Transfusion Information Security Task Force, Bobos A, Boecker W, Childers R, Couture A, Davis R, *et al*. ISBT guidelines for information security in transfusion medicine. Vox Sang 2006;91:S1-23.