Data Management in the ART Laboratory: Requirements and Solutions

66

Timothy Brown and Bruce R. Gilbert

Abstract

The assisted reproductive laboratory has unique requirements for data management. There is a constant stream of data from both the andrology and embryology laboratories as well as those from reference laboratories. There is also quality control (QC) and quality assurance (QA) tests that need to be done at specified times with the results constantly being monitored by the laboratory staff. In addition, much of these data points need to be both entered and accessed in real time in a secure and verifiable way. Then, of course, there is the need for reporting on this data for clinical decisions, patient discussions, and to satisfy regulatory requirements. These requirements for our database solution create the need for a complex management solution. The challenge for database developers is to program all these features in the background and create a user interface that is simple and intuitive. This chapter discusses the basic components of a database design and the special concerns for the assisted reproductive technologies (ART) laboratory. We also introduce key terminology for discussions with developers. Our intent is to present information that will allow the reader to understand the essentials of data management, specific concerns for the ART laboratory, and current regulatory issues in order to better evaluate their current or future database solution.

Keywords

Database management solutions • Assisted reproductive technologies laboratory data • Tissue banking database • *Chain of custody* tracking of tissue • Data confidentiality in the ART laboratory

The assisted reproductive laboratory has unique requirements for data management. There is a constant stream of data from both the andrology and embryology laboratories as well as those from reference laboratories. There is also quality control (QC) and quality assurance (QA) tests that need to be done at specified times with the results constantly being monitored by the laboratory staff. In addition, much of these data points need to be both entered and accessed in real time in a secure and verifiable way. Then, of course, is the need for reporting on this data for clinical decisions, patient discussions, and to satisfy regulatory requirements. These requirements for our database solution create the need for a complex management solution. The challenge for database developers is to program all these features in the background and create a user interface that is simple and intuitive.

This chapter discusses the basic components of a database design and the special concerns for the assisted reproductive technologies (ART) laboratory. We also introduce key

T. Brown, BA, MBA
LifeLab Solutions, Inc., 900 Northern Blvd., Suite 230,
Great Neck, NY 11021, USA
e-mail: Tim@lifelabsolutions.com

B.R. Gilbert, MD, PhD, HCLD (✉)
Professor of Urology, Hofstra North Shore LIJ School of Medicine,
Great Neck, NY, USA

Director, Reproductive and Sexual Medicine, Smith Institute
for Urology, North Shore LIJ Health System, Great Neck, NY, USA
e-mail: bgilber@nshs.edu

Z.P. Nagy et al. (eds.), *Practical Manual of In Vitro Fertilization: Advanced Methods and Novel Devices*,
DOI 10.1007/978-1-4419-1780-5_66,

terminology for discussions with developers. Our intent is to present information that will allow the reader to understand the essentials of data management, specific concerns for the ART laboratory, and current regulatory issues in order to better evaluate their current or future database solution.

Databases

A database is a software tool to store data in such a manner that the data can be entered and recalled easily, securely, and reliably. Initially, word processors or spreadsheets were used to store information. However, users quickly outgrew this because such information is difficult to search and update as the quantity of data multiplies exponentially. A database provides the framework to store such information as data elements, so the user can easily access it. However, it is up to the user to design the framework of the database so that it allows ease of data entry and ease of data recall.

For example, let us say you receive a monthly summary of all your patients' lab results as values in a spreadsheet. How would you find the history of a single patient's lab values for the past 2 years? To do this using your spreadsheet, you would need to open up the 24 spreadsheets you have received and find the results of this single patient and then copy the values and place it into another spreadsheet to show the history. That would be, to say the least, time-consuming. However, if the database framework was designed to include the patient name, date of lab test, and name of the lab test, the user would only need to query the database (fancy word for find) for these values for a specific patient name, and the data would instantly be returned.

A database is therefore an integrated collection of logically related records or files consolidated into a common pool that provides data for one or more multiple uses. The database stores, manages, and retrieves data via the use of tables. If you are familiar with spreadsheets, then you may unknowingly be familiar with what a table is and therefore how databases are structured. A worksheet represents a table, and each worksheet can have many columns (fields) and rows (records). Like a spreadsheet, a database can have many worksheets (tables).

The way data is stored in a database is really important in order to retrieve and report on such data. In general terms, every time we see a patient, we do not create a new patient chart, we just add new information to the chart. The same logical progression occurs with a database. It gets better. A well-designed database will allow us not only to view the patient records but also to cross-reference this patient with other like patients. We also do not have to fill out repeating information each time we enter new data on a patient. For example, patient demographic information only needs to be entered once for a patient since it has been previously entered into the database.

There is, however, an important caveat. The value of the information recalled from a database is only as good as the information entered into the database. A well-designed and normalized database can prevent input of erroneous data by incorporating what is termed business logic. Business logic, built into the database through a process known as programming, provides a database with intelligence. It requires the database to act in a defined way. For example, when we are entering a new patient to the database, we might want to require the following fields to be completed: first name, last name, address, date of birth, and medical record number. If anyone of these fields is not completed on data entry, then we can write a short program, often termed a script, to report this error to the user. The programming, or built-in logic, can be quite different depending on the patient population. Take for instance a field containing the date of birth. If all our patients are adults, we might require that this field must be between 18 and 120 years. However, for a pediatric patient population, the logic might be between 0 and 18 years. In the end, what the business logic does is based on your particular needs.

There are less than a hundred companies that design database platforms: mySQL, Oracle, DB2, Microsoft SQL, PostgreSQL, Access, FileMaker, and 4D are a few of the large platforms offered. There are thousands of companies that create solutions for customers based on these database platforms. Almost all of these databases use Structured Query Language (SQL) to store and retrieve data. To be able to view this data, you need a user interface. There are two principle types of user interfaces, graphical user interface (GUI) and Web-based user interface (WUI). There are numerous programs that developers utilize to create a user interface.

Interoperability

ART laboratories utilize a multitude of software systems. These might include practice management systems (PMS), electronic health records (EHR), and laboratory information systems (LIS), as well as multiple data streams entering their facility from outside laboratories and regulatory agencies. The ability for these systems to talk to each other is extremely important. Doing so saves staff time by reducing the need to enter the same data in multiple systems and allowing for real-time access to data, as well as providing for a single interface for all data. Interoperability [1] is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged." In order to achieve interoperability between systems, there must be a standard language the systems can understand. The standard used in health care is called "HL7." There are two version of this standard being employed by institutions, version 2.x and

version 3.x. The majority of messaging being employed today uses version 2.x. There has been a slow adoption rate of the newer version 3.x standard created in 1995.

Many systems on the market are HL7 compliant. In other words, they can accept and transmit HL7 messages between other HL7 compliant systems. It is important to know what version they support to know the interoperability with other systems. Although HL7 transactions are a standard, implementation is certainly not turnkey. The HL7 standard provides 80% of the framework for implementation, leaving the other 20% for a customized interface. This customized portion is where a software developer can spend a considerable amount of time building the interface.

System integration is often confused with system interface. There is a significant difference between the two and is relevant to HL7 transactions. If two systems are *integrated*, that generally means the data is only stored in one system and is accessed by the other system. With system integration, there is no confusion as to what is the current data. When systems are *interfaced*, the data is replicated from one system to the other, and therefore, there is more than one source for that data. Having the same data in multiple places, as occurs when systems are interfaced, can cause data to be out of sync, causing confusion on what is the most current data.

ART Laboratory-Specific Concerns

Reproductive Tissue Storage

All ART laboratories need to manage the storage tanks that contain reproductive tissues (sperm, oocytes, and embryos). Good clinical practice (GCP), as well as many regulatory agencies, requires *chain of custody* tracking of the movement of vessels stored in these tanks. In software jargon, this is referred to as an audit trail. This can be done electronically or on paper. However, any system you implement needs to document multiple data points each time a vessel (i.e., vial or straw) is moved, used, destroyed, or released. There also needs to be rules for identifying the transaction and verifying the user's privileges for that transaction, meaning that only authorized personnel should be able to perform functions in the system that is within their scope of work. When receiving vessels from another lab, store the receiving labs demographic and tissue information. When receiving sperm vessels, the sperm analysis should be entered into the system if available. This allows easy comparison to the sperm processing once used.

Your standard operating procedure manual (SOP) will need to be reviewed and revised based on the business logic of the software you selected. This is often overlooked, but it is critical that the SOP and software solution are consistent. For example, if, prior to implementing a software system that manages the specimens in tanks, the rules are that a lab technician can prepare the vessels to be sent and the lab director must sign the release form prior to placement in the Release Binder. The new rule may be that the lab director must electronically sign the database record *prior* to the release of the vessel.

The tracking of media that touches any reproductive tissue is regulated. Each time a solution (e.g., media or reagent) comes in contact with the reproductive tissue, that solution needs to be identified and tracked along with the vessel. This entails tracking a number of data points, for example, media name, manufacturer, lot number, date of receipt, and date of expiration, to name a few. The ability to quickly find the vessels and corresponding patients associated with a given solution lot number is particularly important in the rare instance of a manufacturer recall.

IVF Cycle Tracking

There is also the need for the IVF cycle itself to be tracked. Medications and lab values for each stimulation day need to be stored within the database. Once oocytes are retrieved, patient retrieval containers need to be verified. In fact, verification occurs at many steps during the IVF cycle and needs to be tracked and achieved for both internal and external audits. This will involve the development of systematic way of organizing the data and providing for verification by a number of staff as specified in the facilities SOP. This organization of data and verification can also be extended to the processes of insemination, retrieval, and transfer, with each of these processes having unique needs. For example, timing the hCG injection and retrieval not only requires following embryo development by ultrasound and hormone levels but also needs to be coordinated with staff and procedure room availability. This can be efficiently managed with real-time processing. The system can also provide for local or remote access to the database by all staff through secure portals.

The use of a sophisticated software solution can also decrease staff time and decrease errors by reducing the multiple entry steps required during the IVF process. One significant way to do this is by entering live data. Avoiding duplication in data entry is paramount. With lab space limited, quick data entry into a tablet PC at the "bench," we have found to be critical to system adoption by the IVF staff. With live bench entry, daily embryo development and grading can be rapidly entered into the database and immediately available to all the IVF staff.

Reporting of IVF data is required by both federal and most state regulatory authorities. In laboratories using paper and pen entry or even spreadsheets, this often takes hundreds if not thousands of staff hours each year to complete. The amount of data required to be tracked and reported on makes

paper and pen or even a standard spreadsheet approach difficult if not impossible to use. It then becomes a manual process to extract the required data for reporting purposes. The time and cost savings of a database solution that has reports scripted to provide the required information on demand are obvious.

Regulatory Reports

The 1992 Fertility Clinic Success Rate and Certification Act [2] requires fertility clinics to file annually the Assisted Reproductive Technology Report (ART Report) with the Centers for Disease Control (CDC). There are two methods of submitting this data to the CDC. Clinics can submit directly to CDC, or if they belong to the Society of Assisted Reproductive Technology (SART) of the American Society of Reproductive Medicine (ASRM), they can enter data to the SART online system. SART then submits their data to the CDC. Many clinics, however, complete this report manually and file with the CDC.

These reports can be submitted through the Internet. However, these reports are complex and require extensive programming and testing to assure accurate transmission of data. Therefore, when reviewing clinical system for your practice, you should make sure that the system being considered can submit data to the agencies that regulate your ART laboratory. Automating those reports can result in substantial savings in staff and financial resources.

Data Access

Having unrestricted access to your own data may seem obvious. However, commercial databases are often "locked down," allowing access to only the areas the vendor allows. This restriction is particularly onerous when you want to make impromptu searches of your data, possibly for a question a patient asked you or for a presentation you need to make. The term "data mining" refers to the process of analyzing data to uncover patterns. Typically, databases are the primary software solution to uncover these patterns. However, many systems do not provide for full access to your data, making data mining difficult. Without this access, your ability to search and report is limited. In addition, the ability to create your own reports is often difficult or impossible without customization by the vendor. Although most database solutions provide for exportation of data to a spreadsheet format (.csv, .exl, etc.), it still requires time and effort on the part of the user and would need to be repeated each time a report is desired. What would be ideal is a dialogue-driven report generator. Most vendors provide consulting services to assist in developing customized dialogue-driven reports. However, the rates for these services are typically higher than that for programming since developing a report requires a working knowledge of the structure of the database as well as the need to test the report for errors. Therefore, it might be well worth the cost to have the vendor create reports that are required.

Regulatory Requirements

A number of federal and state regulatory requirements need to be considered when evaluating software systems. These include the Health Insurance and Portability Accountability Act of 1996 (HIPAA) [3, 4], HITECH Act of 2009 [5], 21 CFR Parts 1270 and 1271, plus state regulations by the Department of Health.

HIPAA Security Rule

The Security Rule is a key part of HIPAA, which was a federal legislation that was passed into law in August 1996 [4]. The Final Rule on Security Standards was issued on February 20, 2003 and took effect on April 21, 2003. Compliance dates were April 21, 2005 for most covered entities and April 21, 2006 for "small health plans" (defined as health plans having annual receipts of $5 million or less). The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all protected health information (PHI) including paper and electronic, the Security Rule deals specifically with electronic protected health information (ePHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. *Administrative Safeguards* refer to policies and procedures designed to clearly show how the entity will comply with the act. *Physical Safeguards* involve controlling physical access to protect against inappropriate access to protected data. *Technical Safeguards* refer to controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

The primary security safeguard that software systems need to satisfy are the technical safeguards. The HIPAA regulations were designed in such a way that compliance can vary from practice to practice, and because of new technology and standards, a system that is compliant today may not be tomorrow. So, what is a practice to do? First, there is no such thing as a compliant or certified system. The Health and Human Services is responsible for enforcing HIPAA regulations. There is no governing body or company entrusted to certify individuals as "HIPAA Certified" or companies or products getting "official HIPAA certification." Therefore, it is up to you to do your homework. Tables 66.1 and 66.2

Table 66.1 Required technical safeguards

1. Access control: implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified
2. Unique user identification: assign a unique name and/or number for identifying and tracking user identity
3. Emergency access procedure: establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency
4. Audit controls: implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information
5. Integrity: implement policies and procedures to protect electronic protected health information from improper alteration or destruction
6. Person or entity authentication: implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed
7. Transmission security: implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network

Table 66.2 Addressable technical safeguards

1. Automatic log off: implement electronic procedures that terminate an electronic session after a predetermined time of inactivity
2. Encryption and decryption (developer): implement a mechanism to encrypt and decrypt electronic protected health information
3. Mechanism to authenticate electronic protected health information: implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner
4. Integrity controls: implement policies and procedures to protect electronic protected health information from improper alteration or destruction
5. Encryption: implement a mechanism to encrypt electronic protected health information whenever deemed appropriate

outline the required and addressable technical safeguards required by the HIPAA Security Rule. Required elements need be implemented in all systems, while the decision to implement the addressable elements is made by the provider. If a provider chooses not to implement an addressable safeguard, he or she needs to document the reasons.

If you desire to create your own system to manage aspects of your practice, make sure you talk with your attorney about the regulations that must be followed.

HITECH Act

Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) [5], enacted as part of the American Recovery and Reinvestment Act of 2009 [6], addresses the privacy and security concerns associated with the electronic transmission of health information. The American Recovery and Reinvestment Act of 2009 was signed into law on February 17, 2009, and established a tiered civil penalty structure for HIPAA violations. There are a number of aspects that affects ART laboratories. This summary will cover how the Act impacts the HIPAA Security Rules and Provider. Areas of interest are protecting ePHI and penalties for security violations.

Civil Penalties

The Act specifies penalties for violations that were eluded to in HIPAA (Table 66.3). A key clarification is that civil penalties can only be imposed in cases of willful neglect, provided the violation is corrected within 30 days.

Criminal Penalties

In June 2005, the US Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA. Covered entities and specified individuals, whom "knowingly" obtain or disclose individually identifiable health information, face a fine of up to $50,000, as well as imprisonment up to 1 year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to 5 years in prison. Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm permit fines of $250,000 and imprisonment for up to 10 years.

Business associates are subject to the same civil and criminal penalties as covered entities for violating these requirements. This exposes technology vendors, practice management companies, transcription services, billing services, attorneys, accountants, and many other types of business associates to direct regulation under HIPAA. This goes into effect 1 year after the law's enactment (February 17, 2010).

Security Breach Notification Rules

As of September 23, 2009, covered entities are mandated to notify affected individuals of a breach involving "unsecured" PHI [7]. The law does not expressly mandate notification to affected individuals of any security breach. Individuals must be notified without "unreasonable delay" and in no event more than 60 days after discovery.

PHI and ePHI

ePHI stands for electronic protected health information. It is any protected health information (PHI) that is created, stored, transmitted, or received electronically. Protected health information (PHI) under HIPAA means any information that identifies an individual and relates to at least one of the following:

- The individual's past, present, or future physical or mental health
- The provision of health care to the individual
- The past, present, or future payment for health care

Table 66.3 Civil penalties

HIPAA violation	Minimum penalty	Maximum penalty
Individual did not know (and by exercising reasonable diligence would not have known) that they violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations. Note: maximum that can be imposed by state attorneys general (regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 mm
HIPAA violation is due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 mm
HIPAA violations are due to willful neglect, but violations are corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 mm
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 mm	$50,000 per violation, with an annual maximum of $1.5 mm

Table 66.4 Eighteen identifiers of protected health information

1.	Name
2.	Address (all geographic subdivisions smaller than state, including street address, city, county, ZIP code)
3.	All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
4.	Telephone numbers
5.	FAX number
6.	E-mail address
7.	Social Security number
8.	Medical record number
9.	Health plan beneficiary number
10.	Account number
11.	Certificate/license number
12.	Any vehicle or other device serial number
13.	Device identifiers or serial numbers
14.	Web URL
15.	Internet Protocol (IP) address numbers
16.	Finger or voice prints
17.	Photographic images
18.	Any other characteristic that could uniquely identify the individual

Information is deemed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity. Data are "individually identifiable" if they include any of the 18 identifiers of PHI (Table 66.4) for an individual or for the individual's employer or family member or if the provider or researcher is aware that the information could be used either alone or in combination with other information to identify an individual.

Instead of removing the data, sometimes, making the information more general is sufficient for deidentification, for example, replacing birth date with an age range.

Encryption of Data

The HITECH Act does not specifically require encryption. However, it clearly states, "Covered entities must comply with the requirements of the HIPAA Privacy and Security Rules by conducting risk analyses and implementing physical, administrative, and technical safeguards that each covered entity determines are reasonable and appropriate." So based on your risk analysis, you may or may not need to encrypt ePHI data. Data stored on devices that are mobile will be at high risk and should be encrypted. These might include:

- Laptop computers
- USB drives (thumb drives)
- Unsecured external hard drives
- Backup media
- Data transmitted via Internet

The HITECH Act defines two types of data with very different definitions and security concerns. These are data at rest and data in motion. Neither the HITECH Act nor the HIPAA regulations defines the type of encryption that should be used, but do mention to use current standards, which would be the encryption standards developed by the National Institute of Standards and Technology (NIST), (Special Publication 800–111; "Guide to Storage Encryption Technologies for End User Devices" Nov. 2007).

Data at Rest

Data at rest is data that resides in databases, file systems, and other structured storage methods. The three methods of securing and encrypting data at rest include full disk encryption, virtual disk and volume encryption, and file/folder encryption. The three methods offer different levels of encryption, the whole hard drive, a volume of a drive, or encryption only at the folder/file level. All three methods only offer protection while the data is at rest and requires the user authentication to decrypt the data.

Data in Motion

Data in motion is data that is moving through a network, including wireless transmission. All network traffic should be encrypted for both wired and wireless access. Many practices implement virtual private networks (VPNs) in order to connect multiple sites or allow users remote access to the office network. Since VPNs can be configured from many different protocols, it becomes complex to generalize about

its characteristics. A VPN provides an encrypted network tunnel between the client computer and the host the network.

Database Validation

Validation Basics

Data validation is the process of ensuring that a database solution operates on clean, correct, and useful data. It uses small programs, often referred to as scripts or routines, to create "validation rules" that check for correctness, meaningfulness, and security of data that are input to the system. The validation rules may be implemented either by comparing what is present in the database to a table of expected results often referred to as a data dictionary or by a program which steps through the data to check validation logic. The HIPAA Security Rule that governs these procedures is 164.312(c)(1) Integrity (Table 66.5). "The facility must implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

This often encompasses authorization, validation, modification controls, and ensuring consistency of data. To facilitate tracking and problem resolution processes,

Table 66.5 IHS HIPAA security checklist

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a
Administrative Safeguards		
164.308(a)(1)(i)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	
164.308(a)(1)(ii)(A)	Has a Risk Analysis been completed IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the Risk Management process been completed IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)	
164.308(a)(2)	**Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.**	COMPLETE
164.308(a)(3)(i)	**Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).**	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine that the Access of an employee to EPHI is appropriate? (A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves you organization or as required by paragraph (a)(3)(ii)(B) of this section? (A)	
164.308(a)(4)(i)	**Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.**	
164.308(a)(4)(ii)(A)	If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect EPHI from the larger organization? (A)	
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? (A)	
164.308(a)(4)(ii)(C)	Have you implemented policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user's right of access to a workstation, transaction, program, or process? (A)	
164.308(a)(5)(i)	**Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).**	
164.308(a)(5)(ii)(A)	Do you provide periodic information security reminders? (A)	
164.308(a)(5)(ii)(B)	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	

(continued)

Table 66.5 (continued)

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a
164.308(a)(5)(ii)(C)	Do you have procedures for monitoring login attempts and reporting discrepancies? (A)	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords? (A)	
164.308(a)(6)(i)	**Security Incident Procedures: Implement policies and procedures to address security incidents.**	
164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or know security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes? (R)	
164.308(a)(7)(i)	**Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.**	
164.308(a)(7)(ii)(A)	Have you established and implemented procedures to create and maintain retrievable exact copies of EPHI? (R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of EPHI data that is stored electronically? (R)	
164.308(a)(7)(ii)(C)	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode? (R)	
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans? (A)	
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? (A)	
164.308(a)(8)	**Have you established a plan for periodic technical and non technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart? (R)**	
164.308(b)(1)	**Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only of the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.**	
164.308(b)(4)	Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances required by paragraph (b)(1) of this section that meets the applicable requirements of Sec. 164.314(a)? (R)	
Physical Safeguards		
164.310(a)(1)	**Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**	
164.310(a)(2)(i)	Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency? (A)	
164.310(a)(2)(ii)	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? (A)	
164.310(a)(2)(iii)	Have you implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision? (A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks)? (A)	
164.310(b)	**Have you implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI? (R)**	
164.310(c)	**Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users? (R)**	
164.310(d)(1)	**Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.**	
164.310(d)(2)(i)	Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? (R)	

(continued)

Table 66.5 (continued)

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a
164.310(d)(2)(ii)	Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? (R)	
164.310(d)(2)(iii)	Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement? (A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of EPHI, when needed, before movement of equipment? (A)	
Technical Safeguards		
164.312(a)(1)	**Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).**	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining for obtaining necessary EPHI during and emergency? (R)	
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt EPHI? (A)	
164.312(b)	**Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI? (R)**	
164.312(c)(1)	**Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.**	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	**Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed? (R)**	
164.312(e)(1)	**Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.**	
164.312(e)(2)(i)	Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of? (A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)	

From http://www.hipaa.ihs.gov/documents/IHS_HIPAA_Security_Checklist.pdf. Accessed 4 December 2010

each interaction with the database must be assigned a unique sequence number or identifier, linking it back to the source:

- Authorization requires that the user must be properly authorized to interact with the database. The process that does this must be tracked and monitored.
- Input data validation requires that the data entered be checked by the system to ensure that it is valid and provides feedback to the user.
- Modification controls require that the system is able to ensure that the system does not have a significant risk of having undetected changes made to the database.
- Consistency of data requires that the system has in place a method to ensure that a user is identified with each data entry or modification of data. This is often done through a separate log file often maintained on a separate computer from which the actual database is located.

Validation Rules

Incorrect data validation can lead to data corruption or a security vulnerability. Data validation checks that data are valid, sensible, reasonable, and secure before they are processed. A validation rule is a criterion used in the process of data validation, carried out after the data has been entered into the database, and involves a validation program based on validation rules. This is to be distinguished from verification. Verification is one aspect of testing a product's fitness for purpose, whereas validation, for our purposes, ensures that our database operates on clean, correct, and useful data. Validation is the complementary aspect. Validation therefore ensures that the data entered is correct, whereas verification checks the integrity of the database.

System validation insures that the LIS manages information well, with the expected accuracy and reliability, file integrity, auditability, and management control [8]. Although

the vendor provides validation during development, it is the end user who is accountable for system validation [8]. Some vendors have voluntarily adopted the ISO 9000 standards of the International Organization for Standardization. However, the International Organization for Standardization is not a certifying body; if a vendor claims to follow its standards, the claim must be certified by a third party.

End-user validation usually involves several steps. An organized approach to validation of a database solution by the end user is presented in detail by Cowan et al. [8]. They describe a five-step process:

1. Identification and description of the system to be validated. To address these issues, the intended function of the system must be specified and documented.
2. Specification of the stage in the system life cycle. A database can be thought of as having a life cycle consisting of several stages. It will be bought, used, upgraded, and perhaps eventually replaced. Validation tasks depend on the cycle stage of the system. These include a definition of requirements phase, a system design specification phase, an implementation phase, a test phase, a checkout phase, and an operation and maintenance phase. Specifying the stage in the system life cycle allows testing and validation to be conducted at distinct points of development of the information system.
3. Development of hazard analyses. Hazard analysis is determination of the potential degree of human harm that might result from the failure of a device or system (i.e., specification of the penalty for failure). This may be as serious as issuing bad data, or it may be minor but annoying, such as printing poor-quality paper reports.
4. Identification of regulatory concerns. This will determine which regulatory agency, if any, will claim jurisdiction and which set of standards will apply to the operation of the system and the validation process. The agencies may include the FDA, state health departments or licensing bodies, and professional accrediting organizations, such as the College of American Pathologists and the Joint Commission on Accreditation of Healthcare Organizations.
5. Documentation. Validation of a system produces a large volume of documentation. These documents include not only the general statements about validation and test plans but also the test scripts and attached listings, screen prints, and test reports, which must include an explicit statement of pass-fail status, the signature of the person conducting the test, and name of the person reviewing the test status and disposition. This documentation must be compiled, organized, and kept in a designated location for management and regulatory review.

Validation is a continual process that needs to be documented in the SOP manual for the laboratory ensuring that a database solution operates on clean, correct, and useful data.

Conclusions

Software systems implemented into an ART laboratory need to be assessed very carefully and deliberately to make sure it not only meets your business goals but also meets regulatory and reporting requirements.

References

1. Nagin VA, Potapov IV, Selishchev SV. Design of acquisition devices management subsystem for IEEE 1073 compliant software agents. Stud Health Technol Inform. 2002;90:774–9.
2. Fertility Clinic Success Rate and Certification Act, Federal Register Notice, 6 Nov 1998 (Vol. 63, No. 215).
3. Department of Health and Human Services. HIPPA Administrative Simplification Regulation Text. 2010. http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf. Accessed 4 Dec 2010.
4. Health Insurance Portability and Accountability Act Of 1996, Public Law 104–191, August 21, 1996. Final rule, Federal Register, Thursday, August 17, 2000 (Vol. 65, No. 160).
5. Health Information Technology for Economic and Clinical Health Act, Federal Register, Monday, April 27, 2009 (Vol. 74, No. 79).
6. American Recovery and Reinvestment Act of 2009, 111th Congress, January 6, 2009.
7. Department of Health and Human Services. Breach Notification Rule. 2010. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. Accessed 4 Dec 2010.
8. Cowan DF, Gray RZ, Campbell B. Validation of the laboratory information system. Arch Pathol Lab Med. 1998;122:239–44.