Washington Health Law Manual — Third Edition
Washington State Society of Healthcare Attorneys (WSSHA)

Chapter 28: Maintenance of Business Records

Author: Laird A. Pisto, JD
Organization: MultiCare Health System

Reference Date: The author prepared this chapter from reference materials that were available as of August 31, 2010.

Biographies

Laird A. Pisto, Author

Laird Pisto has served as Associate General Counsel to MultiCare Health System since 2000, providing transactional and risk management support to MultiCare's four acute care hospitals, outpatient surgery centers and extensive ancillary service programs, as well as its Health Information Management, Information Services and EPIC Application Service Provider (Community Electronic Health Record) programs. He works extensively with its Corporate Compliance and Internal Audit, Finance, HIPAA Privacy & Security, Anti-Fraud, Patient Safety, Human Resources, Human Subjects Research and Risk Management/Quality Improvement teams.

Mr. Pisto is a frequent speaker on health law, health technology, risk management and corporate compliance matters. He has presented at many events sponsored by AHLA, WSSHA, AHIMA and WHCRMS, as well as Association of Corporate Counsel (formerly ACCA,) American Bar Association and Canadian Bar Association events in the United States and Canada, and CLE events sponsored by the Washington State Bar Association, Seattle-King County Bar Association, Pierce County Bar Association and Seattle University School of Law.

Prior to joining MultiCare, Mr. Pisto served as counsel to Catholic Health Initiatives (Franciscan Health System) and as General Counsel to Care Computer Systems, a nationwide provider of software for the long term care industry (now a part of Keane.) As a shareholder and partner with the firm Hollowell, Pisto, Kalenius & Rhodes, PS during the first half of his legal career, he was engaged in a general civil practice which evolved over time into a general civil trial practice.

Mr. Pisto received his BA from the University of Utah in Journalism and Political Science in 1973, and a JD from the Seattle University School of Law in 1979.

Acknowledgments. The following individuals contributed to research, content, and editing of this chapter:

- Megan Stanley, Seattle University School of Law, 2010 Extern
- Benjamin Miller, University of Washington School of Law, 2010 Extern
- Rebecca Quasney, Seattle University School of Law, 2010 Extern
- Jenni Hanna, University of Washington School of Law, 2010 Extern
- Paul Westfall, Seattle University School of Law, 2009 Extern
- Kristi Wood, Seattle University School of Law, 2008 Extern
- Darryl Colman, Gonzaga Law School, 2008 Extern
- Don Tulanon, Seattle University School of Law, 2007 Extern
- Carlene Brady, Seattle University School of Law, 2006 Extern

Chapter Outline

28.1 Overview: Reasons for Implementing a Document Retention Program

28.1.1 What is a Document Retention Program?

There is an old adage in healthcare that "if it wasn't documented, it didn't happen." Variations on this theme play out in every industry. Document retention programs are designed to ensure that information needed to conduct the business of the company is maintained and retained for such periods of time as may be required for business purposes or longer periods of time as may be mandated by governmental, regulatory or industry standards.

What is a record? In its simplest form, a record is information recorded in some form because there is a likely need for it in the future. A record has also been described[1] as any "document" in any physical or electronic form that contains:

- Content -- the information the document contains.
- Context -- shows such things as intended use, purpose or recipients.
- Structure --its appearance, physical layout or record type.

And, another way of thinking about what constitutes a "record" is to consider a record to be any recording of data, information, knowledge and/or wisdom by one individual that is understandable by another.

Records may be "static" or "transient" in nature. Static records are those that are created once, and never change. Transient records are constantly evolving. One example of this might be a daily temperature log, coupled with an average temperature table. The log will never change once a temperature is recorded, while the table is changing with every new entry.

In these materials, the terms "Document" and "Record" are synonymous. Records and/or Documents in any form or format are considered to be the same throughout these discussions, without regard to their origin and/or the media in which they were created, scanned, emailed, stored or retained. This is not to say that one should not fully understand the nature and origin of any document or record held or maintained by an organization.

28.1.2 Why a Document Retention Program Matters to Your Business

90% of the businesses who have lost substantially all of their records because of a disaster never reopen their doors. Think about the impact of a fire, flood, or earthquake on your business operations.

One-third of the trillion dollar cost of health care delivery in the United States is devoted to creating and processing information. What percentage of the costs of conducting your business is devoted to knowledge and information management?

Twenty years ago, there were estimated to be roughly 400 billion documents managed by US business. Today, that number is estimated to exceed two trillion documents. There is more information available on the internet today than existed in all of the libraries in the world less than 100 years ago. In the last 30 years, more information was produced than in the preceding 5000 years, with an expected rate of doubling every five years. (Moore's Law?)

19 copies of each document produced by a business are made, on average. Of these 8 are completely unnecessary, 10 are stored duplicates and 17 of the 19 are never referred to again. 95% of all references to

[1] Dietel, et. al., *Designing an Effective Records Retention Compliance Program*, Thomson West 2002, Volume 3, Corporate Compliance Series, at 1-11.

records are to those less than 3 years old. And estimates show that between 70% and 90% of all record retrievals are to records less than 18 months old.

As a result of the foregoing, it is important that any assessment of a document retention program consider both the quality of the information being recorded and maintained, as well as whether needed information is being properly acquired and added to the program?

28.1.3 Goals and Objectives of a Document Retention Program

Given the broad definition of what a record is, and the even broader implications of state and federal laws applicable to business records, it becomes important for businesses to fully understand what "records" are kept and maintained by the business, and how long such records "must" be maintained, and in what form. Positive "Preventive Law" strategies can assist any entity in maintaining and demonstrating compliance. Formalized records retention practices impose a certain discipline upon all members of an organization, and help to formulate expectations around how the organization is managed. Examples of this are Enron / Arthur Andersen, both cases in which the ethics of the organization matched closely the document retention practices of the organization, leading to chaos, loss of control and ultimately the downfall of each of these preeminent organizations.

A properly developed and consistently maintained document retention program can provide enormous value to any enterprise. Competitive advantages can be derived through:

- Lower cost
- Higher quality
- Faster delivery
- Excellent service
- Innovation

Records are often the sole source of "institutional memory" in an organization. For example:

- In the "1927 deed from XYZ Church, were there any restrictions as to the use of the property conveyed?"
- Did the Board approve the Employee Retirement Plan prior to the filing of the Federal Tax Return in 19XX?
- Was the ABC Department authorized to dispose of the sales records from Texas that were transferred here when you closed the Dallas office?

Records retention programs run between two extremes:

- Save Everything Forever
- Save Nothing Longer Than Legally Mandated

Between these two extremes lies common sense. Neither of the "extreme" approaches is workable, and neither will be perceived to add value to an organization.

Just as retaining documents for the "right" amount of time can be important to demonstrate compliance, risk develops from keeping records for an inordinate or unnecessary duration. Consider that:

- Most corporate information systems are clogged and overflowing (i.e. email in-basket?)
- Information overload is the most common complaint of managers and workers alike.
- Too many records increase the likelihood of error in accessing "correct" information.
- The most dangerous threat to a company's security and records are "insiders." The longer information is retained, the more likely it may travel in unwanted directions.
- More information is lost through accident and negligence than through sabotage.
- More than 80% of filed records are never referred to again, and 40% have absolutely no value.
- Fire contributes to 90% of records lost each year.

The Records Retention Program developed should:

- Be an integral part of the entity's objectives (Mission, Vision, Values)
- Protect the entity from legal risk, administrative agency criticism and oversight agency concern
- Contribute to the management and success of the enterprise
- Reflect the ethics and values of the organization
- Add value

28.1.4 Overview of Statutory Requirements and Applicable Law

Records are controlled by a myriad of federal and state statutes, implementing regulations and industry guidelines or standards that may have been voluntarily adopted (or mandated) by an entity's commitment to follow such guidelines or practices. More specific presentations concerning various record types will be given by others as part of today's presentations. Suffice it to say that reconciling state and federal records retention requirements can be difficult and confusing. Added to this, the State and federal evidentiary rules applicable to your business may further mandate certain retention practices, particularly in circumstances where litigation (actual or threatened) is involved. Failure to comply with applicable court rules pertaining to document retention and preservation practices can result in extraordinary harm to the corporation, both from a public relations perspective as well as a litigation strategy perspective.

28.2 Record Types – Why Does it Matter?

28.2.1 Sarbanes-Oxley

28.2.1.1 Introduction

The Sarbanes-Oxley Act of 2002, also called the Public Company Accounting Reform and Investor Protection Act ("Sarbanes-Oxley") was enacted in response to corporate accounting scandals, notably Enron, WorldCom, and Tyco. In essence, Sarbanes-Oxley imposes new accounting and financial reporting requirements on publically traded companies to promote corporate transparency, and to restore public trust in America's corporate sector. Sarbanes-Oxley also substantially increases the penalties for securities fraud and makes it a federal crime to alter, cover up, falsify, or destroy any document to prevent its use in an official proceeding.

Although most health systems are nonprofit entities and therefore not explicitly required to comply with Sarbanes-Oxley, many nonprofits have voluntarily opted to adopt policies and procedures in the spirit of the Act: to promote honesty and transparency in board governance. Further, two sections of Sarbanes-Oxley apply to all entities, including nonprofits. One of these is Section 1107, which provides protection for whistleblowers by making it a felony to retaliate against an individual for providing law enforcement authorities with truthful information relating to the commission, or probably commission, or possible commission or any federal offense. The other section, relevant to this chapter, is Section 802 and relates to document retention and destruction.

Because all health systems must comply with Section 802 of Sarbanes-Oxley, it is important to adopt a document retention and destruction policy that complies with the Act. The following provides basic guidelines for implementing Sarbanes-Oxley compliant document retention policies and procedures. It is divided into three parts: Part One will provide an overview of how Sarbanes-Oxley relates to record retention, and some best practices for a compliant document retention policy; Section Two will provide a general schedule listing the time periods for which some types of documents must be retained to comply with the Act; Section Three will provide links to helpful resources.

28.2.1.2 Section One

Section 802 of Sarbanes-Oxley makes it a crime to knowingly alter, destroy, mutilate, conceal, cover up, falsify, or make a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence a legal investigation (e.g., a federal investigation, or a bankruptcy proceeding). Violators may be fined and/or imprisoned for up to 20 years.

By imposing these penalties, Sarbanes-Oxley turns intentional document destruction into a process that must be monitored, justified, and carefully administered to guarantee compliance. This process becomes

even more complicated because Sarbanes-Oxley adopts a very broad definition of "records." Under the Act, a record may be any material that contains information about the entity's plans, results, policies, or performance. In sum, virtually anything about the entity that can be represented with words or numbers could be considered a record, and therefore must be maintained and/or destroyed in accordance with Sarbanes-Oxley.

It is obvious that individuals, nonprofit organizations, and companies alike all need to shred or otherwise dispose of unnecessary or outdated files. Further, common sense and responsible business practices dictate that all entities need to maintain appropriate records about their operations. For example, employment records, financial records, contracts, real estate records, and records of other major transactions are most likely already archived according to existing guidelines established by the entity.

Because all health systems have extensive documents, having a written, mandatory document retention/destruction policy is very important. Such a policy serves to limit accidental document destruction, simplifies external audits, and sets the procedure in case of federal investigation or litigation.

28.2.1.3 Recommendations

To comply with Sarbanes-Oxley, the document retention policy should do the following:

- Address which records are kept or destroyed (originals, photocopies, duplicates with changes noted, drafts, notes, memoranda…);
- Establish a retention period for each type of record;
- Assign responsibility for the enforcement of the policy within the organization;
- Include guidelines for handling electronic files and voicemail, because such records have the same status as paper files in litigation-related cases. These records include, but are not limited to,
  - Emails
  - Internet browser information
  - Instant messages/chat records
  - Voicemail
  - Text messages
  - Blogs/social media
- Contain an exclusion from the policy for litigation or audit purposes;
- Provide procedures to implement and amend the policy; and
- Provide backup procedures.

Sarbanes-Oxley also has sections targeted toward ensuring accuracy of financial disclosures. One of these is section 302. Under 302, the company officer who signs certifies that he or she is "responsible for establishing and maintaining internal controls" and "have designed such controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared."

These internal controls are further evaluated under Section 404 of Sarbanes-Oxley, which requires management and the external auditor to file a report on the adequacy of the company's internal controls over financial reporting. Under 404, management must produce an internal control report assessing the effectiveness of the internal controls and procedures in place at the company.

Under Sarbanes-Oxley, external auditors, as part of their audits, are also required to assess the internal controls in place at the company. These provisions of Sarbanes-Oxley have bearing on Document Retention programs because any "record" that contains information pertinent to the company's financial reports must be maintained and easily accessed.

28.2.1.4 Section 2

As discussed above, the federal government considers just about any type of company information as a business record, and must be retained for a minimum period of time. The following is a sample of various types of documents, and their generally accepted retention periods:

- Accounts payable ledger 7 years
- Accounts receivable ledger 7 years
- Audit reports of accountants Permanently
- Bank statements 7 years
- Capital stock and bond records Permanently
- Charts of accounts Permanently
- Contracts and leases Permanently
- Correspondence (legal) Permanently
- Deeds, mortgages, bill of sale Permanently
- Employee payroll records Permanently
- Employment applications 3 years
- Inventories of products 7 years
- Insurance records Permanently
- Invoices to customers 5 years
- Invoices from vendors 5 years
- Patents Permanently
- Payroll records and tax returns 7 years
- Purchase orders 5 years
- Safety records 6 years
- Time cards and daily reports 7 years
- Training manuals Permanently
- Union agreements Permanently

This list is not all-inclusive and there are hundreds of other documents types that may factor into an investigation or legal action. Under Sarbanes-Oxley, such records must be searchable and quickly available upon request.

28.2.1.5 Section Three

Additional resources include the following:

- The Sarbanes-Oxley Act and Implications for Nonprofit Organizations, BoardSource and Independent Sector, revised in January 2006. Available at http://www.boardsource.org/clientfiles/sarbanes-oxley.pdf.

- Eileen Morgan Johnson and Dorothy Deng, Record Retention and Document Destruction Policy for Nonprofit Organizations, Whiteford Taylor & Preston, LLP. Available at http://www.far-roundtable.org/luncheon/documents/Record-Retention_Policy_Handout.pdf.

- The Record Retention Guide, The Massachusetts Society of Certified Public Accountants, Inc., Federal Taxation Committee, 2004. Available at http://www.cpa.net/resources/retengde.pdf.

- Summary of the Sarbanes-Oxley Act available at www.aicpa.org/sarbanes/index.asp.

28.2.2 US Patriot Act

The US Patriot Act contains numerous provisions that grant the government the authority to access employees records, for instance voicemail and email information. Although the Patriot Act does not contain specific

provisions addressing document retention, a document retention program that addresses those types of transient data is prudent and useful to ensure speedy compliance with the Patriot Act.

28.3 Conducting An Inventory

28.3.1 Assessing Current Document Retention Program

In order to ascertain your ability to implement a litigation hold on internal documents and records within your organization, you may wish to conduct an internal readiness assessment in order to determine and resolve any gaps. Recent changes to the Federal Rules of Civil Procedure, and corresponding provisions of applicable laws and regulations such as Sarbanes-Oxley (SOX) mandate that we be able to readily identify all relevant electronic documents pertaining to known or threatened litigation, and that we be able to impose a hold on such documents to ensure they are not inadvertently lost or destroyed during the pendency of such matters. Similar rules apply in the context of state or federal governmental audits.

Your organization likely already maintains and routinely updates a document retention schedule. See sample document retention schedule (**APPENDIX A**), which is intended to impose a minimum duration of retention for each type of record maintained within the system. However, known or threatened litigation or audits would automatically extend the document retention timeline through the conclusion of such matters.

The following is intended to assist you in developing additional information pertaining to each type of electronic record maintained by your organization, so that you can assess your ability to impose a litigation hold on specific records, should the need arise.

28.3.2 Sample Tool for Assessing Current Document Retention Program

28.3.2.1 Identification of electronic systems in use today

Within each department, which types of electronic record systems are used? By way of example, does your department maintain the following?:

- Primary Electronic Records Systems
- Recovery / Backup / Secondary Systems
- Transient Systems (i.e. systems that are being closed down, that may no longer be used, but which may contain data relevant to your department.)
- Overlapping / Duplicative Data
- Hand-Helds, PDAs, Blackberry Devices
- Removable drives (thumb drives)
- External hard drives
- Home computers
- Internet & Intranet Sites / Workgroups
- Third Party Records Systems, such as:
  - Employees
  - Agents
  - Contractors
  - Vendors
  - Trade Organizations
  - Quality Oversight Agencies
  - Auditors
  - Regulators

28.3.2.2 Assessment of the Current Document Retention Plan

- For each source of data identified, do you have a document retention plan in place?

- Does your retention plan match the relevant Document Retention Policy?
- Do you have data or documents that are not identified within the Document Retention Policy by document type? Please describe in sufficient detail to allow those documents to be added to the policy.
- Is there a staff person in your department whose line responsibility includes management of the Document Retention Policy as it pertains to your department?
- Do you train employees on your Document Retention Policy?

28.3.2.3 Implementing a Litigation Hold

- Could your department, independently, impose a litigation hold on each type of electronic record you maintain?
- Has this been tested?
- Who would the point person be for executing a litigation hold? Is this part of their assigned job title and established area of responsibility?
- If a litigation hold is placed, where would the relevant documents be maintained during a litigation hold? How would they be identified as being subject to such a hold? How would they be differentiated from other routine documents maintained in your department?
- Who has the authority to release a litigation hold? Is there an established process? Is the process documented contemporaneously with the release of the hold?

28.3.2.4 Document & Record Destruction Practices

- Does your department currently destroy or erase records that are no longer required under the Document Retention Policy?
- If so, who within your department is responsible for document destruction?
- How do you track and record the destruction of records and files?
- Is there a practice of inquiring about pending claims and audits built into your document destruction plan?
- Is the person responsible for document destruction the same as the person responsible for implementing a litigation hold in your department?

28.3.2.5 Hardware & Software Retention Requirements

- For each type of electronic record maintained in your department, consider the following:
- What computer hardware is required to gain access to your data?
- What specific software is required? Proprietary?
- Is a particular operating system required?
- Who is responsible for maintaining working tools necessary to view your data electronically?
- Who is responsible for maintaining licenses to any necessary software?
- Is there a hardware / software retention schedule defined? For example, if the Document Retention Schedule imposes a 20 year retention schedule for your data, do you have a plan for maintaining access to the necessary equipment needed to support the schedule?
- Is there a data migration plan in place for software no longer in use?

- Will it be feasible to display your electronic data in its native format if needed? For example, if you use EPIC and your records are in EPIC, "native format" would mean viewing the data using the EPIC system on hardware compatible with EPIC.

28.3.2.6 Building a Metadata Library

- Metadata is "data about your data." The simplest example would be a Microsoft Word document. If you look into the tab "File" and then "Properties" you will see "data about your document" such as the name of the author, date created, date modified, last printout, etc.
- Do you maintain a library of metadata regarding your systems and the information you routinely collect in your department?
- Who is responsible for the metadata?
- Where is it kept?
- How often is it updated?

28.3.2.7 Use of Third Party Vendors / Resources

- Is your department dependent upon third party vendors for the support or maintenance of your data systems?
- If so, who are they, and are they under contract?
- Are those vendors aware of the document retention practices applicable to the data they manage?
- Do you maintain an active contact list for each vendor?
- Would they be required to participate in any form of litigation hold process? Could you perform a litigation hold without their assistance?

28.3.2.8 Current Practices Regarding Backup Tapes / Disks / Devices

- Does your department maintain its own backup systems? Or are your backups performed by other personnel? Or third parties?
- Have you tested the "restore" process using your backup tapes or devices as the source data?
- How long are your backup materials kept? For example, if you use tapes, how frequently are they overwritten?
- Can you call for specific files within your backup system? Or does your backup require a full system restore in order to retrieve individual files?
- What is the expected useful life of your backup media? Is that life longer than your required document retention period for the data in question?
- Are your backup materials "sequential" or "complete sets?" For example, can you restore your entire system from the most recent single set of backup materials? Or must you have access to multiple sets in order to fully restore?
- Where are your backup sets kept? Is someone specifically assigned to the task of maintaining these sets and rotating them? Part of their job responsibilities?
- Do you use or access any form of internet based remote backup or off-site storage process? If so, who knows about those resources? Who has access? Passwords? Log-in codes?

- Do you encrypt your backup tapes, disks or other devices? Are they password protected? If so, who has access? Where are passwords and log-in materials kept?

28.3.2.9 Use of Mobile Devices, PDAs, Portable Computers, Etc.

- Do you use any form of mobile computing devices in your department?
- Are they company-owned devices or personally owned by the user?
- Are they approved by the relevant departments to be used in conjunction with proprietary or confidential information, protected health information or other confidential data owned or controlled by the employer?
- Is access password protected? Is the data encrypted? If lost or stolen, can the data be scrubbed or erased remotely?
- Do others access the device(s) routinely? i.e. Spouse, children, co-workers? Others?
- Do you audit the data kept on such devices? Are files and materials routinely purged or erased when no longer needed? How is this monitored?

28.3.2.10 Use of Email Accounts

- Do your departmental employees each manage their own email accounts?
- Do you provide guidance to departmental employees regarding how they should manage their employer-run email accounts? If so, is that guidance consistent with the Document Retention Policy?
- Do you audit departmental employees concerning their use and retention of email?
- Do your departmental staff use personal email accounts for business purposes?
- If so, are those accounts maintained by the department or the individual?
- Do you migrate data from those email accounts into employer-run systems?
- How do you distinguish work-related emails from private emails?
- Do your employees use any form of instant messaging as part of their work?
- If so, are your employees provided any guidance regarding the use of instant messaging for work-related purposes?
- Do you retain copies of instant messages? If so, where are those stored?

28.3.2.11 Other Concerns or Issues

Do you worry about any of your data or document retention practices? What concerns you? What do we need to know? Where are fixes required?

28.4 Designing and Maintaining an effective Document Retention Program

28.4.1 Establishing Guidelines for Document Destruction

Guidelines for document destruction are available through many resources. National organizations such as:

- American Health Information Management Association
- Internal Revenue Service
- Association of Corporate Counsel – Model Corporate Records Retention Guidelines
- Secretary of State (i.e. Washington Secretary of State) and State Departments such as Washington Department of Licensing
- National Organizations of Many Types, i.e.

  - Trade Associations (Just about any large industry group provides guidelines for trade-specific record groups.)
  - National Accounting and Audit Firms.
  - Consulting firms (every industry, every type.)
- Document Retention Consultants
- Books (both general and industry-specific)
- University of Washington electronic reference: http://f2.washington.edu/fm/recmgt/retentionschedules/gs/general/uwgs5

Each entity should closely compare any lists or guidelines with an internally developed list of documents and document types used routinely within the organization. A cross-walk should be developed to match up each document type used within the organization with a corresponding and confirmed external benchmark or guideline.

Those familiar with this process will confirm that there will likely be discrepancies between any two sets of guideline materials or industry recommendations. Those who have been "saved" by a long dead document will likely advocate for longer retention periods, while those who have been "burned" by a smoking gun will advocate for destroying documents as soon as possible. In between, you will find statutory minimum retention periods and common sense to guide you.

Attached to this Chapter is a sample Records Retention Guideline from the University of Texas that demonstrates a relatively complex program with careful assignment of roles among a large population of program administrators. See, APPENDIX A. Larger organizations retain so many documents that it may be impossible to monitor any program without a reference list of this type. As can be seen from the Appendix, there are numerous other policies referenced, such as the "Storage (Retention) Policy" which contains line items for each type of document maintained by the university.

Smaller organizations may feel comfortable assigning retention periods by document category, as opposed to "type." In those circumstances the discretion of each manager is called upon to correctly identify the category and type of each record and to understand the potential interdependence between and among various record types and record categories within the larger inventory.

28.4.2 Implementing a Program

No records retention program will be perfect beyond the instant of its creation. Recommended retention periods, record types, formats, and business needs, as well as business constraints, will constantly evolve, leaving any program to play catch-up with the real world of the business. The important thing about any program is to simply "get started." You are likely already doing it – if for no other reason than you may work in an office where they have "never thrown anything away, ever."

In developing a program, consider the following common characteristics of business information:

- Accuracy, completeness and availability determine information value.
- Information loses value over time.
- Management of information requires "cradle to grave" thinking, with specified life plans for each record type.
- When business needs change, retention periods change.
- The value of information may depend upon the existence of other information. Information often gains value in the context of other information.
- When information is linked, the length of time it should be kept will change.

- Some information can simply be replaced or updated rather than retained.
- Information must be of some use or potential reuse to have value.

28.4.3 Department and Personnel Involved

Records management programs intrinsically involve "nearly everyone" in the organization, at some level. Traditionally, records management was afforded little in the way of assets, a small percentage of management oversight, and very small budgets.

Today, organizations have begun to recognize the importance of their data. By way of example, in a service-oriented society (as compared to a manufacturing society) the value of the organization's data far exceeds anything physically produced by the organization. Likewise, the loss, destruction, theft, damage or destruction of the core data of the organization could imperil the very survival of the organization or its competitive advantage. Consequently, as the value of data increases, one would expect that the level of oversight of the records retention process and how the life of data is managed within the organization would rise to a level commensurate with the value of the assets being managed and protected.

Fundamentally, the Records Retention Program will be given professional status and recognition as an integral part of the organization, with appropriate allocation of assets and funding necessary to achieve the goals of the program over the life of the organization. A comprehensive corporate records management program will involve Board-level oversight, with routine interaction and visibility before the Audit Committee and other appropriate internal and external auditors.

28.4.4 Program Manager and Document Retention Committee

One would expect any Records Retention Committee to include:

- Legal representation
- Operations representation from each core area of the business
- Assigned "ownership" and "responsibility" for all functions of the program
- Audit representation from the Corporate Compliance / Internal Audit side
- Oversight by VP or higher levels of the organization's leadership
- Annual Board-level reports on the efficacy of the program

Because each individual department or business unit is likely to have ownership or operational control over only a small part of the total records program, it is also advisable to consider appointment of one or more individuals within the organization with primary accountability for the program. In larger organizations, this may fall on Finance, Accounting, Internal Audit, Legal or some other defined department. In smaller organizations, the function will likely be absorbed by the Chief Cook & Bottle Washer.

Without regard to the level of sophistication of the organization, corporate records personnel should demonstrate:

- Knowledge and understanding of the organization's Mission, Vision and Values
- Thorough understanding of where the corporation is at present, and where the leadership is steering the organization
- Ability to anticipate the information needs of the organization and its officers and directors
- Ability to distinguish useful information from "data"
- Professional competence in evaluating and recommending "best practices" in terms of technology and best practices surrounding the information assets of the organization

- Thorough understanding of the technologies in place and the mechanics of document management and retrieval
- Desire to achieve "best practices" status for the organization
- The ability to integrate and actively practice each of the foregoing skills

28.4.5 Monitoring Compliance

There should be a systematic and progressive records audit and evaluation program conducted at appropriate intervals (not to exceed five years) in which a full self-assessment of the efficacy and appropriateness of the plan is evaluated and the program is updated to include any new media or processes, as well as to determine any archival requirements for technologies reaching the end of their life cycle. Interim compliance audits (routine annual program reviews with comments) can be coupled with operational changes that may require adjustments to the program. By way of example:

- How many floppy disks do you have in your archives?
- How many floppy disk drives do you have in operation?
- How many dot-matrix printers do you have in your inventory?
- Where are your tape drives residing these days?
- Does your microfiche reader have a light bulb installed?

As with any "service" provided (internally or externally) one can measure the success of the service line through establishment of a set of key criteria that customers use to measure satisfaction, including:

- Dependability, accuracy, reliability, timeliness
- Assurance, locus of control, confidence
- Perceptual indicators
- Willingness, responsiveness, caring manner
- Concern, empathy, equity, attention to customer's needs

Keep in mind the old adage: "That which you measure improves."

28.4.6 Impending Litigation

Your organization will get no better chance to demonstrate its compliance than will arise through "almost any" meaningful litigation. No matter what type of lawsuit you become involved in, you are almost certain to face a variety of discovery requests which will test the mettle of the most well-developed document retention program.

One of the key elements of any document retention program will be the ability of the organization to orchestrate a proper "litigation hold." This simply means that at the instant that a lawsuit is threatened, known or "reasonably certain" to arise from a chain of events, the organization can immediately suspend all routine document destruction processes, so as to ensure that no documents relevant to the litigation are lost or destroyed through inadvertent failure to notify "all" relevant personnel, third parties, agents and corporate leaders of the need to retain such materials through the duration of the litigation.

Many cases that might otherwise have been won in court were "lost" when the court determined that corporate personnel had either willfully and intentionally destroyed documents or evidence, or had simply neglected to protect and preserve documents that "might" have made a difference in the outcome of a case. In such cases, courts have imposed "default judgments" against parties, leaving the only question for trial to be the amount of damages owed by the offending party to the litigation.

28.4.7 Importance of Following Established Policies

No better guidance in the utility of following your established Record Retention Policies can be found than that set forth in the Federal Sentencing Guidelines, which became effective in 1991. These guidelines provide federal courts with sentencing ranges for various crimes, many of which fall into the category of "white collar" crime, such as tax offenses, fraud, antitrust, etc. Within the Sentencing Guideline is this comment on *Culpability*:

> …Culpability generally will be determined by the steps taken by the organization prior to the offense to prevent and detect criminal conduct, the level and extent of involvement in or tolerance of the offense by certain personnel, and the organization's actions after the offense has been committed…

An appropriately established, formally adopted and routinely maintained Records Retention Program will protect the organization by minimizing the likelihood of a crime being conducted and by increasing the likelihood of detection of any crime, allowing the organization to properly report any wrongdoing.

Beyond state and federal criminal sanctions, a comprehensive program will enable the organization to demonstrate compliance with any of the thousands of potentially applicable state or federal laws, rules or contractual obligations incumbent upon the organization, and to gather those records which will most likely enable the organization to defend itself from claims.

Regularly maintained business records of any organization are the records "most likely" to protect an organization from spurious litigation, and/or to minimize damages in instances where appropriate claims are brought. Oftentimes, the mere "absence" of a record that would otherwise ordinarily have been kept by a party will be sufficient to tip the balance in favor of the other party to litigation (the inference being that the record must have been damaging, or it would have been produced.)

28.4.8 Resources and Acknowledgements

Much of the content of this Chapter is inspired by the substance and text of a (very!) comprehensive manual on records retention program design entitled: *Designing an Effective Records Retention Compliance Program* by J. Edwin Dietel, JD (Senior Official, Central Intelligence Agency (Ret'd) together with Senior Advisors Joseph E. Murphy, Exec. VP, Legal Systems Legal Group, and Paul H. Dawes, JD, Latham & Watkins, SFO.), published by Thomson West in 2002 as Volume 3 of the Corporate Compliance Series. For those developing a complex corporate records retention program, or who have been assigned responsibility for managing any complex program, you are highly encouraged to obtain the full text of this publication plus the myriad appendices accompanying it.

A number of Business Records Industry Associations & Societies have resources regarding document retention and management. A number of these are referenced below.

- (Browser search on any of these)
- Administrative Management Society
- American Management Association
- Association for Information & Image Management
- Association for Information Management
- Association for Systems Management
- Association of Commercial Records Centers
- Association of Information Processing Professionals
- Association of Records Managers & Administrators
- Business Systems & Security Management Association

- Data Management Association
- Institute of Certified Records Managers
- International Information Management Congress
- International Records Management Council
- National Assoc. of Government Archives & Record Administrators
- National Records Management Council
- Office Automation Management Association
- Society for the Advancement of Management
- Society for Information Management Systems
- Society for Management Information Systems
- Society of American Archivists

The following resources are useful document retention resources:

Washington State Health Care Specific:

1) Washington State Health Public Hospital District Record and Retention Schedule from the Washington State Archives (March 2009): http://www.sos.wa.gov/_assets/archives/Public%20Hospital%20District%20%20RRS%2Over%204.0%20rev.pdf.

2) Washington State Health Departments and Districts Record and Retention Schedule from the Washington State Archives (March 2009): http://www.sos.wa.gov/_assets/archives/Health%20Departments%20and%20Districts%20RRS%20ver%203.0%20rev.pdf.

3) Washington State Department of Health Medical Quality Assurance Commission Guidelines on Retention of Medical Records when Closing a Practice (July 2005): http://www.doh.wa.gov/hsqa/MQAC/Files/MedRecordReten.pdf.

Washington State Specific:

4) Washington State Records Retention Schedules can be found at: http://www.sos.wa.gov/archives/RecordsRetentionSchedules.aspx.

5) University of Washington General Records Retention Schedule: http://www.f2.washington.edu/fm/recmgt/sites/default/files/General%20Schedule%20Rev%2011%20Web%20version.pdf.

Health Care Specific:

6) AHIMA (American Health Information Management Association) retention schedule and general recommendations: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_012545.hcsp?dDocName=bok1_012545.

7) Document Retention Schedules taken from HCA (Hospital Corporation of America): http://ec.hcahealthcare.com/CPM/ADMRetSch.pdf.

8) Example Policy taken from Alliance for Children and Families website: http://www.alliance1.org/magazine/Summer2008/retnetion.pdf.

9) Compilation of recommendations on retention schedules, from Access Information Management, a document management company: http://www.accessyourdocs.com/RetentionSchedule--Medical?1137037955.pdf.

10) University of Pennsylvania Record Retention Schedule Health Administration Records (2002): http://www.archives.upenn.edu/urc/recrdret/healthadminall.html.

11) Joel Wakefield, *Document Retention: A Quick Reference Guide*, 37 J. Health L. 493 (2004)

12) Article documenting records retention practices in US hospitals (2008): http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2430773/.

General/Miscellaneous:

13) Oregon University System Record Retention Schedule (2003): http://libweb.uoregon.edu/records/schedule/166-475-0095.html#18.

14) Internal Revenue Services, guidelines on records retention from Compliance Guide for 501©(3) organizations (2000): http://www.irs.gov/pub/irs-pdf/p4221pc.pdf.

15) Deloitte, LLP (DTT) (consulting firm), guidelines and recommended retention periods (2009): http://www.deloitt.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/Retention%20of%20Doc%202003(3).pdf.

Other Sites With Restricted Access:

16) AHLA (American Health Lawyers Association)(password protected).

17) AHA (American Hospital Association)(password protected).

18) WSHA (Washington State Hospital Association).

19) WSMA (Washington State Medical Association)(other than closing practice).

20) The Joint Commission (only a general statement about state law, regulation, patient care needs).

21) The Association of Corporate Counsel has a link to a model policy, but it requires a password and per the website, is up to date as of 2001 (pre SOX)(http://www.acc.com/search.cfm).

22) Association for Information and Image Management website has an article on developing a records retention schedule but it is only accessible to members: http://www.aiim.org/infonomics/abcs-of-records-retention-schedule-development.aspx.

28.4.9 Sample Document Management and Retention Policy with Schedule

See APPENDIX A attached hereto.

28.5 Defining the Record Set

28.5.1 What is a Medical Record

28.5.1.1 Definition: Medical Record

A “Medical Record” is defined as a chronological written account of a patient's examination and treatment that includes the patient's medical history and complaints, the physician's physical findings, the results of diagnostic tests and procedures, and medications and therapeutic procedures. See, The American Heritage Stedman's Medical Dictionary, 2nd Edition, 2004.

Historically, the "medical record" of a patient consisted simply of those documented entries contained within a defined paper chart labeled with the patient's name, prepared, stored and maintained within each of the various health care entities and providers who saw the patient.

With the advent of computerized patient records and the expanded interchange and exchange of individually identifiable health information among providers and other care-related organizations, payor groups, employers, and others, it has become a necessity to more carefully analyze and define exactly "what is the medical record?"

An excellent starting point is a short article on this topic, entitled "Definition of the Health Record for Legal Purposes" by Margret Amatayakul, et. al., which can be found at the AHIMA website: http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_009223.html, Journal of AHIMA 72, no.9 (2001): 88A-H. See also: *A Practical Assessment Guide*. Washington Health Information Management Association and Health Information Technology Committee, November 1, 1997.

This Chapter does not attempt to replicate those materials, but for those who have yet to craft a complete definition of your Designated Record Set under HIPAA, the foregoing resources are extremely useful and will save you countless hours in reinventing the wheel.

28.5.1.2 Definition: Health and Medical Information

RCW 70.02.010 includes the following definitions for health and medical information:

- (6) "Health care information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information.
- (4) "Health care" means any care, service, or procedure provided by a health care provider: (a) To diagnose, treat, or maintain a patient's physical or mental condition; or (b) That affects the structure or any function of the human body.
- (8) "Health care provider" means a person who is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession.

28.5.1.3 Definition: Billing and Business Information

RCW 70.02.010 includes the following definitions related to billing and business information:

- (12) "Payment" means:

  (a) The activities undertaken by: (i) A third-party payor to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits by the third-party payor; or (ii) A health care provider, health care facility, or third-party payor, to obtain or provide reimbursement for the provision of health care; and

  (b) The activities in (a) of this subsection that relate to the patient to whom health care is provided and that include, but are not limited to:

  (i) Determinations of eligibility or coverage, including coordination of benefits or the determination of cost-sharing amounts, and adjudication or subrogation of health benefit claims;

  (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

  (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, including stop-loss insurance and excess of loss insurance, and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following health care information relating to collection of premiums or reimbursement:

(A) Name and address;
(B) Date of birth;
(C) Social security number;
D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider, health care facility, and/or third-party payor.

28.5.1.4 Definition: Designated Record Set Under HIPAA[2]

Under HIPAA, a designated record set is defined as follows:

A group of records maintained by or for a covered entity that is:

The medical records and billing records about individuals maintained by or for a covered health care provider;

The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

Used, in whole or in part, by or for the covered entity to make decisions about individuals.

For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. See Hughes, Gwen, "Practice Brief: Defining the Designated Record Set" found at: http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_017122.html, Journal of AHIMA 74, no.1 (2003): 64A-D.

A comprehensive HIPAA Preemption Analysis of Washington laws and their relationship with HIPAA is available through the Washington State Hospital Association located at www.wsha.org. Each statute referencing PHI under Washington law has the potential to limit or modify access rights otherwise granted under HIPAA, requiring careful consideration as to whether existing Washington law is more restrictive than HIPAA.

28.5.1.5 What is NOT Part of the Medical Record?

HIPAA generally permits disclosures by a covered entity for purposes of Treatment, Payment and Operations (TPO)[i]. Recent amendments to the UHCIA bring the Washington provisions into close alignment with HIPAA's federal mandates.

It is important to recognize that the definitions and limitations inherent to the use and disclosure of TPO under HIPAA are in essence the "heart and soul" of HIPAA for the average provider. If a use or disclosure fits clearly within one of the TPO definitions, the provider need not account for, track, document or otherwise worry about such uses and disclosures. These definitions create a safe harbor for many, if not most, routine health care operational activities and functions.

[2] 45 CFR § 164.501

28.5.1.6 Definition: Treatment.

The term "treatment" is defined as follows:

- the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party;
- consultation between health care providers relating to a patient; or
- the referral of a patient for health care from one health care provider to another.

28.5.1.7 Definition: Payment.

The term "payment" is defined as follows:

- Determining eligibility or coverage under a plan
- Adjudicating claims
- Risk adjustments
- Billing & Collection
- Reviewing health care services for medical necessity, coverage, justification of charges
- Utilization review
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his/her payment history and identifying information about the covered entity.

28.5.1.8 Definition: Operations.

Operations" means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

- Conducting Quality Assessment and Improvement Activities, including:
  - outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;
  - population-based activities relating to improving health or reducing health care costs
  - protocol development
  - case management and care coordination
  - contacting of health care providers and patients with information about treatment alternatives
  - related functions that do not include treatment.
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities.
- Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess loss insurance), provided that the requirements of Section 164.514(g) are met [restricting uses and disclosures by recipients.]

- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs.
- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.
- Business management and general administrative activities of the entity, including but not limited to:
  - Management activities relating to implementation of and compliance with HIPAA
  - Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor or customer
  - Resolution of internal grievances
  - Sale or transfer, merger or consolidation of all or part of a covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity
  - Consistent with the applicable requirements of Section 164.514, creating de-identified health information and fundraising for the benefit of the covered entity.

The following definitions of health care operations under the UHCIA are now consistent with the foregoing HIPAA provisions:

> (7) "Health care operations" means any of the following activities of a health care provider, health care facility, or third-party payor to the extent that the activities are related to functions that make an entity a health care provider, a health care facility, or a third-party payor:
>
> (a) Conducting: Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, if the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
>
> (b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance and third-party payor performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of nonhealth care professionals, accreditation, certification, licensing, or credentialing activities;
>
> (c) Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care, including stop-loss insurance and excess of loss insurance, if any applicable legal requirements are met;
>
> (d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
>
> (e) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the health care facility or third-party payor, including formulary development and administration, development, or improvement of methods of payment or coverage policies; and
>
> (f) Business management and general administrative activities of the health care facility, health care provider, or third-party payor including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this chapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that health care information is not disclosed to such policy holder, plan sponsor, or customer;

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of a health care provider, health care facility, or third-party payor with another health care provider, health care facility, or third-party payor or an entity that following such activity will become a health care provider, health care facility, or third-party payor, and due diligence related to such activity; and

(v) Consistent with applicable legal requirements, creating deidentified health care information or a limited dataset and fund-raising for the benefit of the health care provider, health care facility, or third-party payor.

The Privacy Rule does not cover information held in an employment file. PHI specifically does not cover employment information maintained by an employer as an employer, for employment purposes. This is consistent with the approach to student medical records, which are covered under FERPA, and explicitly excluded from the definition of PHI. But, it should be noted that the "Employment" exception applies only to PHI held in the role of "employer." Any PHI derived while carrying out its health plan or health provider functions, is fully protected PHI and comes under the act.

For those entities covered by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) the Management of Information Standards (IM) speak directly to the organization's charting requirements. See, for example, the following sections of the Comprehensive Accreditation Manual for Hospitals (CAMH):

Patient-Specific Information[3]

IM.6.10 The hospital has a complete and accurate medical record for every individual assessed, cared for, treated, or served.

IM.6.20 Records contain patient-specific information, as appropriate, to the care, treatment, and services provided.

IM.6.30 The medical record thoroughly documents operative or other high-risk procedures and the use of moderate or deep sedation or anesthesia.

IM.6.40 For patients receiving continuing ambulatory care services, the medical record contains a summary list of all significant diagnoses, procedures, drug allergies, and medications.

IM.6.50 Designated qualified personnel accept and transcribe verbal orders from authorized individuals.

IM.6.60 The hospital can provide access to all relevant information from a patient's record when needed for use in patient care, treatment, and services.

[3] The Comprehensive Accreditation Manual for Hospitals (CAMH) and all content, including the identified standards, are the property of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO.) CAMH and its contents are subject to copyright and trademark protection of JCAHO.

Examples of statutory charting obligations arise from provisions such as RCW 70.41.190, which specifies the process for retention and preservation of medical records, and which provides that the Department of Health (DOH) "shall by regulation define the type of records and the information required to be included in the medical records to be retained and preserved under this section, . . ." The DOH, through the Washington Administrative Code (WAC) then promulgates regulations such as those found at WAC 246-320-205.

28.5.1.9.1 WAC 246-320-205

WAC 246-320-205 states the following:

> The purpose of the management of information section is to obtain, manage, and use information to improve patient outcomes and the performance of the hospital in patient care, governance, management, and support services. Hospitals will:
>
> 1) Facilitate patient care by providing medical staff and other practitioners timely access to information systems, resources, and services;
>
> 2) Maintain confidentiality, security, and integrity of data and information;
>
> 3) Initiate and maintain a medical record for every individual assessed or treated including a process to review records for completeness, accuracy, and timeliness.
>
> Medical records must:
> a) Contain information to identify the patient, the patient's clinical data to support the diagnosis, course and results of treatment, author identification, consent documents, and promote continuity of care;
>
> b) Be accurately written, dated, timed, promptly filed, retained in accordance with RCW 70.41.190 and chapter 5.46 RCW, and accessible;
>
> c) Indicate: i) The legally authorized practitioner authenticated the medical record after the record was transcribed; and ii) Entries are dated and authenticated in a timely manner;
>
> d) Include verbal orders by authorized individuals which are accepted and transcribed by qualified personnel;
>
> 4) Establish a systematic method for identifying each medical record(s) to allow ready identification of area of service, filing, and retrieval of all the patient's record(s); and
>
> 5) Adopt and implement policies and procedures that address: a) Access to and release of confidential data in medical records in accordance with chapter 70.02 RCW; and b) Transmittal of pertinent medical data to ensure continuity of care.

28.5.1.10 HIPAA and State Law Security Concerns

The Washington UHCIA includes specific requirements for security safeguards,[4] which require that the hospital implant "reasonable safeguards for the security of all health care information it maintains." Separately, HIPAA mandates that effective April 21, 2005, each hospital must:

[4] RCW 70.02.150

- Implement reasonable and appropriate administrative, technical, and physical safeguards that ensure the confidentiality, integrity, and availability of the electronic PHI they collect, maintain, create, or transmit;
- Protect against reasonably foreseeable threats to the security or integrity of the information;
- Protect against any reasonably anticipated uses or disclosures of the information that are not permitted by the Privacy Standards; and
- Ensure that its workforce comply.

Among the factors that hospitals must consider when determining appropriate "reasonable" security safeguards:

- The hospital's size, complexity, and capabilities (scalability);
- Its technical infrastructure, hardware, and software security capabilities;
- Costs of the security measures; and
- The probability and criticality of potential risk to electronic PHI.

The prevailing standard at this time appears to be "as secure as is feasible for the covered entity." As a large covered entity, hospitals likely will not get the 'benefit of the doubt' with respect to foreseeable violations of privacy or security by outside members of its medical staff (and their support staff) who are afforded access to PHI via the EHR. Thus, appropriate insurance and indemnity provisions applicable to third-party usage must be factored in.[5]

28.5.2 HIPAA Compliance: Defining the Sample Health System Designated Record Set

<table>
<tr><td rowspan="2">SAMPLE HEALTH CARE SYSTEM</td><td colspan="2">Effective date signifies approval of this SHS policy by the Quality Leadership Council</td></tr>
<tr><td colspan="2">Policy No.</td></tr>
<tr><td rowspan="4">Subject:

1 HIPAA Compliance: Defining the Sample Health System Designated Record Set</td><td>Effective Date:
9/03</td><td>Page
1 of 6</td></tr>
<tr><td>Date of Origin:
5/03</td><td>Review Date:
9/05</td></tr>
<tr><td>Point of Contact:
HIM</td><td>Telephone Number:</td></tr>
<tr><td colspan="2">Proponent: HIM
PHI Workgroup</td></tr>
</table>

[5] John Christiansen, a long-time WSSHA member, in conjunction with the AHLA, has recently published an extensive monograph on data security, *An Integrated Standard of Care for Healthcare Information Security: Risk Management, HIPAA, and Beyond* available through AHLA at: http://ahla.org/Ecommerce/ProductDisplay.cfm?ProductID=71569 And separately, AHLA has produced numerous publications regarding the HIPAA Security Standards. See, for example: *Security Standards - (HIT Practice Group Member Price) (Electronic)* By Marilyn Lamar, Esq., M. Peter Adler, Esq., Dean W. Harvey, Esq., and Richard D. Marks, Esq., also available at the AHLA site.

- Purpose: To establish the Sample Health System (SHS) policy and procedure that defines standard for the SHS Designated Record Set, set forth in the Privacy Rule, Section 164.524. This rule states that individuals generally have a right to inspect and obtain a copy of protected health information (PHI) about them in a designated record set.
- Policy: SHS personnel will only disclose to authorized individuals and entities document types in the SHS designated record set in this policy.
- References:
  - SHS Policy – HIPAA Compliance
  - SHS Policy – Records Management and Retention
- Definitions: Designated Record Set (DRS) - is defined as a group of records maintained by or for a covered entity that is:
  - the medical and billing records about individuals maintained by or for a covered healthcare provider
  - the enrollment, payment, claim adjudication, and case or medical management record systems maintained by or for a health plan or information used in whole or part by or for the covered entity to make decisions about individuals.
  - Examples of Protected Health Information included and excluded in the designated record set are set forth in the attached Appendix.
- Procedures:
  - All SHS personnel will review the SHS Designated Record Set addendum
  - Prior to disclosing protected health information review the addendum so the appropriate information may be disclosed.
  - Contact the Privacy Office if you have questions on what is in the SHS Designated Record Set.
- Forms:
  - Protected Health Information included in the SHS Designated Record Set
  - Protected Health Information excluded in the SHS Designated Record Set

Examples of content per SHS Policy Records Management and Retention Policy

SHS Designated Record Set	Examples
Medical record of covered providers	The content of paper based inpatient medical records. Examples of content per SHS Policy Records Management and Retention Policy for: Allenmore Mary Bridge Tacoma General Printed copies of the Intensive Care Electronic Record (CareVue in adult ICU, Centricity in PICU)
	The content of paper based outpatient records. Examples of content per SHS Policy Records Management and Retention Policy for: Hematology/Oncology charts

SHS Designated Record Set	Examples
	Obstetrics records Ambulatory Surgery charts Home Health records Hospice Records Community Child Maternal Clinic CAID
	The information defined as the legal health record in a computer based record environment. Examples of content per SHS Policy on Records Management and Retention Policy for: EpicCare Centricity CareVue LastWord
Other records used to make decisions about the individual	Photographs, EKG strips, EEG reports etc.
	Copies of reports and records generated by other providers, example: outside records. A History and Physical generated by a physician at a hospital and incorporated into the resident's record in a long term facility because it will be used to make decisions about the individual. Copies of reports generated by other providers used to make decisions about an individual, even when such records are kept in a separate location or file folder Example Physical Therapy records CAID Records
	E-mail communications that have been printed and placed in the paper or electronic record
Records maintained by a business associate that meet the definition of designated record set that are not merely duplicates of information maintained by covered entities	Records maintained by records storage companies that have agreed to manage release of information rather than returning the records to the covered entity to respond Example – Iron Mountain Storage Center and SourceCorp Copy Service

Protected Health Information Included in the SHS Designated Record Set

Billing records of covered providers	The content of a patient account file in a paper based office or computer based environment, such as patient specific claims, remittance, eligibility response charge screen, statement of account balance and payment agreement, Consent and authorization forms, Medicare ABN letter, Medicare Life Time Reserve Letter, Medicare Notice of Non-Coverage and copy of insurance card. Examples: HCFA form, UBS, new or old account histories, print screen of transactions, copies of pharmacy history and billing records, inpatient and outpatient billing records
The enrollment, payment, claims. adjudication, and case or medical management record systems maintained by or for a health plan	The information defined as enrollment, payment, claims, adjudication, and case or medical management in a health plan environment. Examples are MMG Denial Letter or Health Plan Denial Letter

Protected Health Information Excluded from the SHS Designated Record Set

Excluded from the Designated Record Set	Examples
Health Information generated collected, or maintained for purposes that do not include decision making about an individual	Data collected and maintained for research, peer review or performance improvement purposes. Appointment and surgery schedules, birth and death registries Diagnosis or operative indexes and duplicate copies of information that can also be located in the individuals' medical or billing record
Psychotherapy notes	The notes of a mental health professional about counseling sessions that are maintained separate and apart for the regular health record
Source Data interpreted or summarized in the individual's medical or health record	Fetal monitors, pathology slides, radiological films, diagnostic films, Video of a surgical procedure,
Other records	E-Mail communications that an organization stores on-line and has not printed out and acted upon
CLIA Clinical Laboratory	Requisitions for laboratory tests and duplicate lab results when the originals are filed in the individuals medical record
Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding	Notes taken by a covered entity during a meeting with the covered entity's attorney about a pending lawsuit
Employer Records	Pre-employment physicals maintained in Human Resources files Results of HIV tests maintained by the Infectious Disease Control Nurse on employees who have suffered needle stick injuries on the job
Business Associate records that meet the definition of designated record set but is merely duplicate information maintained by the covered entity	Transcribed reports that have been transmitted to the covered entity. Examples: in-house and outsourced transcription services
Education Records	Records generated and maintained by teachers and teacher aides employed by a school district or an institution for developmentally disabled
Individually identifiable health information maintained by an organization that are not covered entities as defined by HIPAA	Medical records in a dental office that maintains all its records and billing systems manually

28.6 Special Issues Surrounding Electronic Records

28.6.1 Electronic Discovery

In 2006 the Federal Rules of Civil Procedure were amended, most notably to alter the rules of electronic discovery. One change was to Rule 34 which was amended to put electronically stored information on the same level as traditional documents. This change is somewhat clarified in Rule 26(b)(2)(B) which divides electronically stored information sources into two categories: (1) ones that are reasonably accessible and (2) ones that are not reasonably accessible. The accessibility of the source is based on whether there is undue burden of cost to retrieving information from the source. Therefore, a party should automatically produce "electronically stored information that is relevant, not privileged, and reasonable accessible, subject to the [Rule 26](b)(2)(C) limitations that apply to all discovery. The new wording in Rule 34 is thus meant to include any metadata which is the information that the computer stores about the creation and alteration of a document. However, in order to receive the metadata the receiving party needs to be sure in request the data in a form that includes metadata, otherwise, the responding party has the choice to produce the electronically stored information in any reasonable form.

These new rules apply to document retention mostly in the form of changing the enforcement of the duty to preserve discoverable information. The duty to search for discovery in reasonably inaccessible electronically

stored information is relieved by Rule 26(b)(2)(B), but that rule does not relieve the party from preserving that inaccessible electronically stored information that is relevant to reasonably anticipated litigation. Since there is so much possibly relevant information that could be stored electronically Rule 37 supplies a "safe harbor." The "safe harbor" is in place not only due to the abundance of information, but also because that information can change periodically without a user's guidance. Therefore, Rule 37(e) was added to protect parties from sanctions due to the "routine, good faith operation of an electronic information system." The advisory committee's note on this rule suggests that "routine operation" of an electronic information system is those actions the system performs without user interference, or the parts of the systems operation that are preset. However, the advisory committee's notes on this rule also indicate that the routine operation of an electronic information system may be required to be suspended or altered to preserve information that might be relevant to reasonably anticipated litigation. The specifics of such a "litigation hold" on electronically stored information, including whether it extends to inaccessible sources of information, needs to be determined on a case-by-case basis according to the Advisory Committee's Notes. Note that this "safe harbor" only applies to sanction under Rule 37.

28.6.2 Emerging Issues Involving Electronic Health Records

It is common for a health care provider to interface with many sources of data related to a single patient. Consider that sources of the EHR may include data from:

- Legacy systems
- Hand-held devices
- Portable electronics
- Imported data
- Imaging systems
- Pharmacy systems
- Laboratory systems
- Home Health systems
- Specialists & Subspecialists
- Multiple community sources

Expansive development of the electronic health record (EHR) is underway. In many instances:

- EHR developments have not kept pace with developing approaches to disclosure in litigation settings.
- Past practices of converting digital records to analog form, and then replicating the chart from the analog form, are becoming passé and arguably improper under developing standards.
- Attempts to produce EHRs in an analog or "print" format present many problems.
- Best practices point toward digital access to EHRs in their native format. But there are numerous obstacles to that path.
- Recent amendments to the Federal Rules of Civil Procedure accelerate the need for assessment of best practices as they relate to the production of electronic health records in litigation settings.

  The struggle we are currently in involves the inability of a single system to fully capture all of the data emerging from these disparate systems. Many providers interface with multiple electronic systems in the course of a single day – often, for example, encountering more than one electronic health record system within a single health care system. It is not uncommon for a provider to encounter multiple electronic systems under one roof, covering the entire spectrum of care delivered by the organization, with separate interfaces for Lab, Pharmacy,

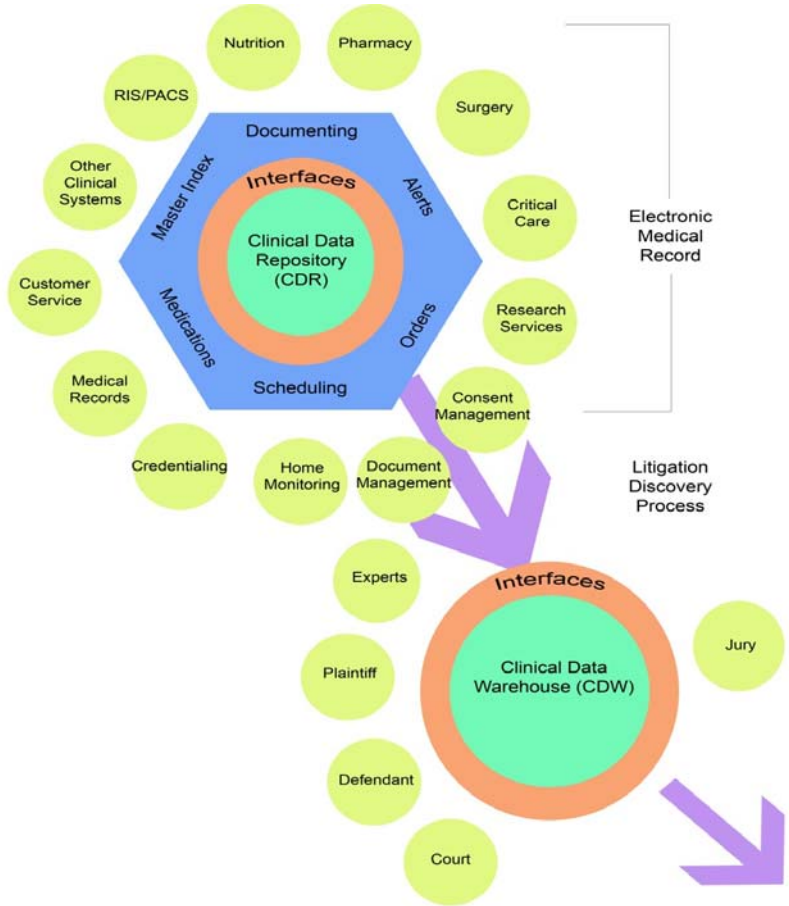
Imaging, Home Health, Intensive Care, Cardiovascular ICU, OR, ED and primary acute care medical records maintained by the organization, often with an additional layer added for the organization's ambulatory care records. This may be complicated further by separate specialized systems supporting pediatric care, oncology, research, or other areas of the care spectrum.

The chart below demonstrates the problem at hand. This model is representative of many health systems, in terms of the architecture of the systems and sub-systems that house elements of a typical health care organization's EHR.

From this chart, one can see that there are many potential collision points between the revised Civil Rules and the EHR in its present state. Each of the upper segments of this chart may:

- Represent separate, stand-alone components of the Legal Medical Record, or Designated Record Set.
- Operate entirely independently of the remaining components
- Be subject to entirely different licensing terms than its peers
- Operate under unique operating systems, interfaces or protocols
- Constitute digital, analog or hybrid record sets

SOURCES OF ELECTRONIC HEALTH RECORD DATA:



Clearly, continued reliance upon historic methods of producing paper / print copies of a patient's electronic medical record in the context of litigation may no longer be warranted.

Further, changes in discovery rules at the federal level are highly likely to be mimicked at the state level in the very near future. Many states already have electronic discovery rules that are substantially similar to the proposed Federal amendments noted above. For these reasons, parties to litigation must proactively plan for electronic discovery as part of the litigation plan and process. Early assessment as to the viability of access to data in its native format should be conducted. As such, these issues must be addressed in any document retention policy.

28.7 Post Destruction Record Keeping

In order to demonstrate routine compliance with document retention and destruction policies and good-faith compliance with litigation hold processes, consideration should be given to maintaining records showing dates and methods of destruction of records. Organizations may have different sensitivities to the detail of record descriptions contained in these record sets, but at a minimum you should be able to demonstrate how and when records were purged from your systems pursuant to the policy. A sample destruction schedule and documentation form is included in the Sample Policy attached (**APPENDIX A**).