

# Electronic Health Record (EHR)

- [Standards](#)
- [Long-term preservation and storage of records](#)
- [Synchronization of records](#)
- [Privacy Concerns](#)
- [Legal issues](#)
  - [Liability](#)
  - [Achieving a Useful Litigation Hold and “Switch Off”](#)
  - [The Duty to Preserve Electronic Medical Records](#)
  - [Legal Interoperability](#)
  - [Customization](#)
  - [Regulatory compliance](#)

## Definition of EHR

An electronic health record (EHR) (also electronic patient record or computerised patient record) is defined as a systematic collection of electronic health information, in digital format, about individual patients or populations, that is capable of being shared across different health care settings, by being embedded in network-connected enterprise-wide information systems. The EHR is generated and maintained within an institution, such as a hospital, integrated delivery network, clinic, or physician office. EHR is a complete record of patient encounters that allows to automate and streamline workflow in health care settings and to increase safety through evidence-based decision support, quality management, and outcomes reporting.

## Advantages of EHR

1. **Reduction of Cost of Health Care;**
2. **Improve quality of care** by help lessen patient sufferance due to medical errors and the inability of analysts to assess quality. For example, Computerized Physician Order Entry (CPOE)—one component of EHR—increases patient safety by listing instructions for physicians to follow when they prescribe drugs to patients. CPOE can tremendously decrease medical errors: CPOE could eliminate 200,000 adverse drug events and save about \$1 billion per year if installed in all hospitals.

3. **Promote evidence-based medicine** by providing access to unprecedented amounts of clinical data for research that can accelerate the level of knowledge of effective medical practices.
4. **Record keeping and mobility** thereby being able to connect to many electronic medical record systems.

### **Disadvantages:**

#### **Start-up costs; Software maintenance costs; Training costs**

1. Physicians who buy the systems may not benefit financially.
2. Physicians tend to see at least short-term decreases in productivity as they implement an EHR and spend more time entering data into an empty EHR.
3. Studies have called into question whether, in real life, EHRs improve quality.
4. Costs: The EHR is costly and there is need to increase information technology staff to maintain the system. [NOTE: The healthcare industry spends only 2% of gross revenues on health information technology HIT, which is low compared to other information intensive industries such as finance, which spend upwards of 10%.]

### **Incentives**

With the [American Recovery and Reinvestment Act of 2009](#), providers were expected to take the full risk of investing in healthcare IT.

The [HITECH Act](#), part of the 2009 economic stimulus package (ARRA) passed by the US Congress, aims at inducing more physicians to adopt EHR. Title IV of the act promises incentive payments to those who adopt and use "certified EHRs" and, eventually, reducing Medicare payments to those who do not use an EHR. Funding for EHR incentives is also added to the [Medicaid](#) system. In order to receive the EHR stimulus money, the HITECH act (ARRA) requires doctors to also show "meaningful use" of an EHR system.

[Health information exchange](#) (HIE) has emerged as a core capability for hospitals and physicians to achieve "meaningful use" and receive stimulus funding. Healthcare vendors are pushing HIE as a way to allow EHR systems to pull disparate data and function on a more interoperable level.

### **Meaningful Use**

The meaningful use of EHRs intended by the US government incentives is categorized as follows:

1. Improve care coordination
2. Reduce healthcare disparities
3. Engage patients and their families
4. Improve population and public health
5. Ensure adequate privacy and security

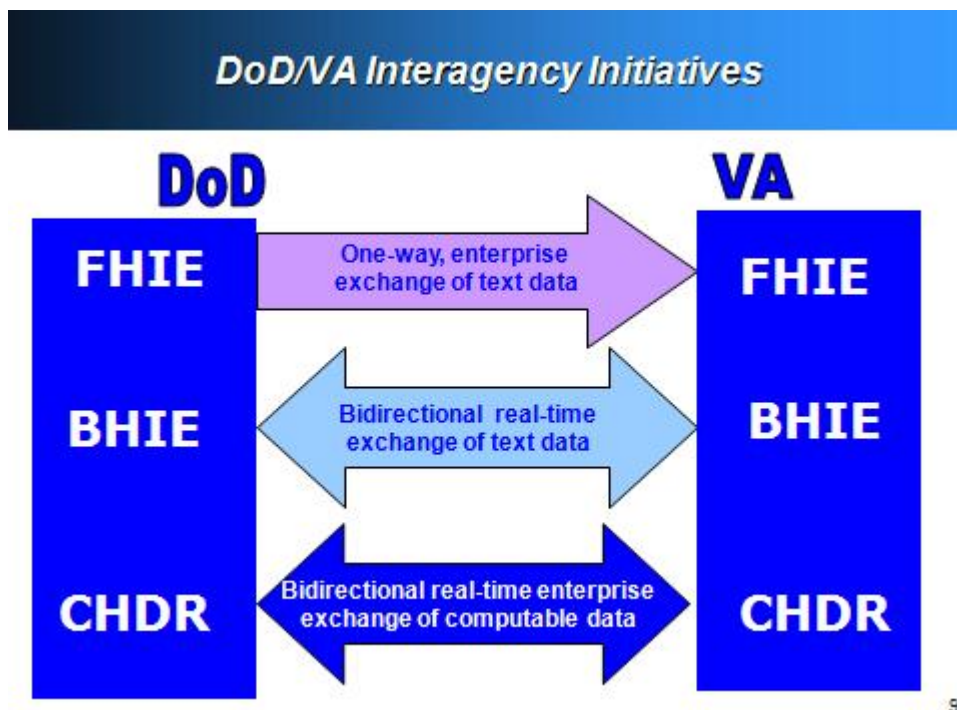
The Obama Administration's Health IT program intends to use federal investments to stimulate the market of electronic health records:

- Incentives: to providers who use IT
- Strict and open standards: To ensure users and sellers of EHRs work towards the same goal
- Certification of software: To provide assurance that the EHRs meet basic quality, safety, and efficiency standards

The detail definition of "meaningful use" is to be rolled out in 3 stages over a period of time until 2015; only stage 1 has been defined.

### Implementations

- In the United States, the [Department of Veterans Affairs](#) (VA) has the largest enterprise-wide health information system that includes an electronic medical record, known as the Veterans Health Information Systems and Technology Architecture ([VistA](#)). A key component in VistA is their [VistA imaging](#) System which provides a comprehensive multimedia data from many specialties, including cardiology, radiology and orthopedics. A [graphical user interface](#) known as the Computerized Patient Record System (CPRS) allows health care providers to review and update a patient's electronic medical record at any of the VA's over 1,000 healthcare facilities. CPRS includes the ability to place orders, including medications, special procedures, X-rays, patient care nursing orders, diets, and laboratory tests.
- The **2003 National Defense Authorization Act (NDAA)** ensured that the VA and DoD would work together to establish a bidirectional exchange of reference quality medical images. Initially, demonstrations were only worked in El Paso, Texas, but capabilities have been expanded to six different locations of VA and DoD facilities. These facilities include VA polytrauma centers in Tampa and Richmond, Denver, North Chicago, Biloxi, and the National Capitol Area medical facilities. Radiological images such as CT scans, MRIs, and x-rays are being shared using the BHIE. Goals of the VA and DoD in the near future are to use several image sharing solutions (VistA Imaging and DoD Picture Archiving & Communications System (PACS) solutions).



9

Clinical Data Repository/Health Data Repository (CDHR) is a program that allows for sharing of patient records, especially allergy and pharmaceutical information, between the Department of Veteran Affairs (VA) and the Department of Defense (DoD) in the United States. The program shares data by translating the various vocabularies of the information being transmitted, allowing all of the VA facilities to access and interpret the patient records. The Laboratory Data Sharing and Interoperability (LDSI) application is a new program being implemented to allow sharing at certain sites between the VA and DoD of "chemistry and hematology laboratory tests." Unlike the CHDR, the LDSI is currently limited in its scope.

One attribute for the start of implementing EHRs in the States is the development of the [Nationwide Health Information Network](#) which is a work in progress and still being developed. This started with the North Carolina Healthcare Information and Communication Alliance founded in 1994 and who received funding from [Department of Health and Human Services](#).

The Department of Veterans Affairs works with Kaiser Permanente to further develop a software which allows to share information with private health care providers. This software called 'CONNECT' uses [Nationwide Health Information Network](#) standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country. CONNECT is an open source software solution that supports electronic health information exchange. The CONNECT initiative is a Federal Health Architecture project that was conceived in 2007 and initially built by 20 various federal

agencies and now comprises more than 500 organizations including federal agencies, states, healthcare providers, insurers, and health IT vendors.<sup>[43]</sup>

The US Indian Health Service uses an EHR similar to VistA called RPMS. VistA Imaging is also being used to integrate images and co-ordinate PACS into the EHR system.

### Standards

- [ANSI X12 \(EDI\)](#) - transaction protocols used for transmitting patient data. Popular in the United States for transmission of [billing](#) data.
- [CEN](#)'s TC/251 provides EHR standards in Europe including:
  - [EN 13606](#), communication standards for EHR information
  - [CONTSYS](#) (EN 13940), supports continuity of care record standardization.
  - [HISA](#) (EN 12967), a services standard for inter-system communication in a clinical information environment.
- [Continuity of Care Record](#) - ASTM International Continuity of Care Record standard
- [DICOM](#) - an international communications protocol standard for representing and transmitting radiology (and other) image-based data, sponsored by [NEMA](#) (National Electrical Manufacturers Association)
- [HL7](#) - a standardized messaging and text communications protocol between hospital and [physician](#) record systems, and between practice management systems
- [ISO](#) - [ISO TC 215](#) provides international technical specifications for EHRs. ISO 18308 describes EHR architectures

### Long-term preservation and storage of records

An important consideration in the process of developing electronic health records is to plan for the long-term preservation and storage of these records. The field will need to come to consensus on the length of time to store EHRs, methods to ensure the future accessibility and compatibility of archived data with yet-to-be developed retrieval systems, and how to ensure the physical and virtual security of the archives.

Additionally, considerations about long-term storage of electronic health records are complicated by the possibility that the records might one day be used longitudinally and integrated across sites of care. Records have the potential to be created, used, edited, and viewed by multiple independent entities. These entities include, but are not limited to, primary care physicians, hospitals, insurance companies, and patients. Mandl et al. have noted that “choices about the structure and ownership of these records will have profound impact on the accessibility and privacy of patient information.”

The required length of storage of an individual electronic health record will depend on national and state regulations, which are subject to change over time. Ruotsalainen and Manning have found that the typical preservation time of patient data varies between 20 and 100 years. In one example of how an EHR archive might function, their research "describes a co-operative trusted notary archive (TNA) which receives health data from different EHR-systems, stores data together with associated meta-information for long periods and distributes EHR-data objects. TNA can store objects in XML-format and prove the integrity of stored data with the help of event records, timestamps and archive e-signatures."

In addition to the TNA archive described by Ruotsalainen and Manning, other combinations of EHR systems and archive systems are possible. Again, overall requirements for the design and security of the system and its archive will vary and must function under ethical and legal principles specific to the time and place.

While it is currently unknown precisely how long EHRs will be preserved, it is certain that length of time will exceed the average shelf-life of paper records. The evolution of technology is such that the programs and systems used to input information will likely not be available to a user who desires to examine archived data. One proposed solution to the challenge of long-term accessibility and usability of data by future systems is to standardize information fields in a time-invariant way, such as with XML language. Olhede and Peterson report that "the basic XML-format has undergone preliminary testing in Europe by a Spri project and been found suitable for EU purposes. Spri has advised the Swedish National Board of Health and Welfare and the Swedish National Archive to issue directives concerning the use of XML as the archive-format for EHCR (Electronic Health Care Record) information."

### Synchronization of records

When care is provided at two different facilities, it may be difficult to update records at both locations in a co-ordinated fashion.

Two models have been used to satisfy this problem: a [centralized data server solution](#), and a peer-to-peer [file synchronization](#) program (as has been developed for other [peer-to-peer networks](#)).

Synchronization programs for distributed storage models, however, are only useful once record standardization has occurred.

Merging of already existing public healthcare databases is a common software challenge. The ability of electronic health record systems to provide this function is a key benefit and can improve healthcare delivery.

### Privacy Concerns

In the United States, the concept of a national centralized server model of healthcare data has been poorly received. Issues of privacy and security in such a model have been of concern.

Recent revelations of "secure" data breaches at centralized data repositories, in banking and other financial institutions, in the retail industry, and from [government databases](#), have caused concern about storing electronic medical records in a central location. Records that are exchanged over the Internet are subject to the same security concerns as any other type of data transaction over the Internet.

The [Health Insurance Portability and Accountability Act \(HIPAA\)](#) was passed in the US in 1996 to establish rules for access, authentications, storage and auditing, and transmittal of electronic medical records. This standard made restrictions for electronic records more stringent than those for paper records.

One major issue that has risen on the privacy of the U.S. network for electronic health records is the strategy to secure the privacy of patients. Former US president Bush called for the creation of networks, but federal investigators report that there is no clear strategy to protect the privacy of patients as the promotions of the electronic medical records expands throughout the United States. In 2007, the Government Accountability Office reports that there is a "jumble of studies and vague policy statements but no overall strategy to ensure that privacy protections would be built into computer networks linking insurers, doctors, hospitals and other health care providers."<sup>[59]</sup>

The privacy threat posed by the interoperability of a national network is a key concern. One of the most vocal critics of EMRs, New York University Professor Jacob M. Appel, has claimed that the number of people who will need to have access to such a truly interoperable national system, which he estimates to be 12 million, will inevitable lead to breaches of privacy on a massive scale. Appel has written that while "hospitals keep careful tabs on who accesses the charts of VIP patients," they are powerless to act against "a meddlesome pharmacist in Alaska" who "looks up the urine toxicology on his daughter's fiance in Florida, to check if the fellow has a cocaine habit." This is a significant barrier for the adoption of an EHR. Accountability among all the parties that are involved in the processing of electronic transactions including the patient, physician office staff, and insurance companies, is the key to successful advancement of the EHR in the U.S. Supporters of EHRs have argued that there needs to be a fundamental shift in "attitudes, awareness, habits, and capabilities in the areas of privacy and security" of individual's health records if adoption of an EHR is to occur.

According to the *Wall Street Journal*, the DHHS takes no action on complaints under HIPAA, and medical records are disclosed under court orders in legal actions such as claims arising

from automobile accidents. HIPAA has special restrictions on psychotherapy records, but psychotherapy records can also be disclosed without the client's knowledge or permission, according to the *Journal*. For example, Patricia Galvin, a lawyer in San Francisco, saw a psychologist at Stanford Hospital & Clinics after her fiance committed suicide. Her therapist had assured her that her records would be confidential. But after she applied for disability benefits, Stanford gave the insurer her therapy notes, and the insurer denied her benefits based on what Galvin claims was a misinterpretation of the notes. Stanford had merged her notes with her general medical record, and the general medical record wasn't covered by HIPAA restrictions.

Within the private sector, many companies are moving forward in the development, establishment and implementation of medical record banks and health information exchange. By law, companies are required to follow all HIPAA standards and adopt the same information-handling practices that have been in effect for the federal government for years. This includes two ideas, standardized formatting of data electronically exchanged and federalization of security and privacy practices among the private sector. Private companies have promised to have "stringent privacy policies and procedures." If protection and security are not part of the systems developed, people will not trust the technology nor will they participate in it.

## Legal issues

### General Liability Issues

In the recent years, healthcare organizations are showing an increased rate of acquisition of computer technologies and their spending rates show an upward tendency placing the industry as one to the major consumers of ICT products and services.

Frost & Sullivan estimates the **Health Information Technology** market (by revenue) in 2008, in APAC (Southeast Asia, China, Japan and Australia) was close to USD5.04 billion with an annual growth rate (CAGR) of 11.8 percent from 2005-2008. Although the APAC HIT market represents currently only 2.1 percent of the total healthcare market, it is very likely that the figure could double if not triple that in the next 10 years.

Dr Pawel Suwinski, senior consultant at Frost & Sullivan says, 'The HIT is here to stay with even more ubiquitous presence in all aspects of healthcare delivery systems. Moreover, it will be the main factor and driver in the transformation of **healthcare industry** towards translation care by providing common collaboration platform for information processing and exchange between related sciences and industries.'

He further elaborates, " 50 percent of the **medical practice** activities can be controlled. The remaining 50 percent depends solely on human judgment and cognitive functions that when unfavourable conditions are present could lead to substandard care. The implementation of HIT can improve the quality of care by providing better control (up to 80 percent). However, while decreasing the legal exposure of traditional medical practice it introduces legal implications related to the usage of HIT."

The following is an introduction of some of the medico-legal aspects of the usage of healthcare IT solutions including electronic medical records.

- **Medical liability** which is also entitled as medical negligence or medical malpractice is a special component of tort law which governs the professional relationship between physicians and their patients. It is concerned about the duties of care expected between physicians and their patients in delivering health care.
  - The duty of a physician to his or her patients is to practice medicine which meets or exceeds the standard of care.
- **Hospital and MCO Liability.** If the hospital or healthcare delivery organizations violate standard of care (through inadequate oversight of its staff physicians) by allowing EHR or other technology of its choice to be used in such a way to harm patients, it might become the subject of corporate negligence action. The case of Vicarious liability occurs when there is a design or other type of flaw in any of the technologies including electronic health record or computerized physician order entry that causes harm to patients even though the physicians or other caregivers who uses that committed no negligence.
- **Unauthorized Access to EHR.** The unauthorized access to patient's private information results in the privacy violation.
  - User negligence, misdirected information flow or intentional security breach by a third party etc..could be some of the reasons for this information leakage.
  - Security breached is recognized as unauthorized sharing of patient's private information.
  - Inappropriate disclosure can happen in clinical setting when multiple copies of **Electronic Health Record (EHR)** persist even after destruction of original file is being accessed by unauthorized personnel.
- Medical liability actions may also arise from **acts of commission which breach the standard of care and result in injury and damages to patients.**
- Physicians could also find themselves in trouble by **failing to use diagnostic and treatment modalities suggested by the embedded best practice guidelines** in

certain types of **electronic health records**. Here there could be an act of omission contributing to patient injury.

- Some of the **preventative measures** suggested in the course of medical liability are:
  - the selection of appropriate **healthcare information system**,
  - proper training of staff to ensure efficient use of system,
  - documenting all information with justification (whether or not care provided), and
  - preventing any further alteration to this records without proper documentation etc..

## **Other Liability Issues**

Legal liability in all aspects of healthcare has been an increasing problem in the United States.

Failure or damages caused during installation or utilization of an EHR system has been feared as a threat in lawsuits. This liability concern was of special concern for small EHR system makers. Some smaller companies may be forced to abandon markets based on the regional liability climate.

Larger EHR providers (or government-sponsored providers of EHRs) are better able to withstand legal assaults.

In some communities, hospitals attempt to standardize EHR systems by providing discounted versions of the hospital's software to local healthcare providers. A challenge to this practice has been raised as being a violation of Stark rules that prohibit hospitals from preferentially assisting community healthcare providers.

In 2006, however, exceptions to the Stark rule were enacted to allow hospitals to furnish software and training to community providers, mostly removing this legal obstacle.

## **Achieving a Useful Litigation Hold**

Kevin F. Brady and Matthew I. Cohen  
The National Law Journal  
July 26, 2005

In the aftermath of the recent \$1.4 billion damages judgment in a case where Morgan Stanley

was sanctioned for its failure to preserve and produce certain electronic records, members of senior management are probably thinking about their company's records retention/destruction policies more than they ever have. Indeed, many general counsel and their staffs are probably spending more time than ever balancing their company's legal obligations to preserve records in the face of litigation with the potentially monumental costs of doing so when relevant electronic data are involved.

While the courts have provided little guidance in this area in the past, the U.S. Supreme Court's recent decision reversing Arthur Andersen's criminal conviction for obstructing a Securities and Exchange Commission proceeding by destroying records immediately before receiving an SEC subpoena, which put the company out of business, offers a new perspective on this situation. While the Court was focused primarily on the standard of culpability for document destruction in the criminal context, there is some language in the Court's opinion that is helpful in the civil context.

The Court acknowledged, for example, the important role that records retention/destruction policies play in corporate operations and noted that "'document retention policies' which are created in part to keep certain information from getting into the hands of others ... are common in business." *Arthur Andersen LLP v. U.S.*, 125 S. Ct. 2129, 2135 (2005) (citation omitted). The Court went on to state that "[i]t is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances." *Id.* Plainly, a company need not suspend the destruction of nonrelevant records in order to comply with its preservation obligations.

A number of recent court decisions involving sanctions for spoliation have focused on companies' efforts to preserve potentially relevant records by examining the "litigation hold" put in place by the companies, and have provided some guidance as to their obligations in this area. A litigation hold, also known as a "preservation order" or "hold order," is a process used by companies to advise their employees of pending or anticipated litigation and of their obligation to preserve relevant records and to suspend their normal records-destruction policies as they relate to potentially relevant records.

A litigation hold is a critical directive that, in many instances, is the company's first line of defense against a "spoliation" claim. While litigation holds set forth specific procedures for employees to follow concerning the preservation of records, one of the most difficult issues for the company to address is how to devise and implement an effective litigation hold that preserves records that are potentially relevant to the litigation and at the same time allows the company to pursue, for legitimate business purposes, the destruction of nonrelevant active and archived data that the company has no business purpose to retain. The answer depends largely on how well the company has prepared for "anticipated litigation." The planning must start well before the litigation arises with a careful analysis of how the company's record-retention policy and its duty to preserve relevant records intersect.

## THE DUTY TO PRESERVE RECORDS

It is well established that the duty to preserve records -- in whatever form -- is triggered when a party learns of pending litigation, "reasonably anticipates" litigation or is put on notice that litigation is imminent. Once the duty to preserve arises, parties must be prepared to take affirmative steps immediately to preserve information that they know or should reasonably know is relevant to the action; is reasonably calculated to lead to the discovery of admissible evidence; is reasonably likely to be requested during discovery; or is the subject of a pending discovery request. See *William T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Calif. 1984); see also *Lewy v. Remington Arms Co.*, 836 F. 2d 1104, 1112-13 (8th Cir. 1987).

These steps should include instituting, as soon as practicable, a litigation hold suspending the destruction of potentially relevant records (including active electronic data) in the ordinary course of business pursuant to the company's record-retention policy and notifying all employees who might have potentially relevant records that the records must be preserved. Companies that fail to take these steps could face serious repercussions.

For example, in *Mosaid Technologies Inc. v. Samsung Electronics Co.*, 348 F. Supp. 2d 332 (D.N.J. 2004), the court found that the defendant, Samsung, did not meet its obligation to preserve and produce potentially relevant e-mails, and awarded the plaintiff monetary sanctions. Further, the court determined that it would issue an adverse-inference instruction to jurors, permitting them to find that the spoliated evidence would have been unfavorable to Samsung.

In granting these sanctions, the court focused on the fact that "Samsung never placed a 'litigation hold' or 'off switch' on its document retention policy concerning e-mail ... [which automatically] allowed e-mails to be deleted, or at least to become inaccessible, on a rolling basis." *Mosaid*, 348 F. Supp. 2d at 333. The court noted the fact that Samsung "knew how to institute a 'litigation hold' and stop the spoliation of e-mails, having done so in one of its divisions in another litigation." *Id.* at 338. The court concluded by stating that "[w]hen the duty to preserve is triggered, it cannot be a defense to a spoliation claim that the party inadvertently failed to [institute] a 'litigation hold' or 'off switch' on its document retention policy to stop the destruction of that evidence." *Id.* at 339.

Companies should implement, as part of their record-retention policy, a litigation rapid response plan that provides a roadmap for the company to quickly identify the types and locations of records-both paper and electronic-in the company's possession, custody or control that are potentially relevant to the litigation or investigation. Just as companies have always had to identify and preserve potentially relevant paper records from their active files, as well as their archival files (offsite storage), companies must identify and preserve electronic records from both active storage systems as well as archival systems, which may include magnetic tape storage, such as backup tapes.

The most critical part of the plan is identifying, capturing and preserving potentially relevant records (in the format in which the records were kept in the normal course of business, if possible). In order to supervise the implementation of the plan, the company should establish a team of dedicated and knowledgeable representatives from the legal, information technology, records management, human resources and finance departments, as well as senior management to spearhead and monitor the implementation of the plan. When litigation or a regulatory investigation is pending or "reasonably anticipated," the team can ensure that the company takes the necessary steps to comply with its preservation obligations (initially, as well as for the long term) in a way that minimizes disruption to the business.

In most cases, it is extremely difficult not only to pinpoint a particular time when litigation is reasonably anticipated, but also to determine with any degree of accuracy the scope of the potential claim -- the causes of action, defenses, counterclaims and crossclaims, and the "key players" related to those pleadings. While the cases that discuss this issue do not specify a particular period of time within which it would be reasonable to implement a litigation hold, they do imply that it should be done "quickly." A delay as brief as a few days can result in spoliation accusations if records are destroyed or if backup tapes are overwritten pursuant to the company's record retention or disaster recovery policies.

However, it may be very difficult, from a corporate perspective, for the entity to determine that litigation is reasonably anticipated. For example, in *Zubulake v. UBS Warburg*, 220 F.R.D. 212, (S.D.N.Y. 2003) (*Zubulake IV*), Judge Shira Scheindlin found that "almost everyone" involved in the case recognized the possibility of litigation and held that the company was on notice. She went on to state, however, that merely because one or two employees contemplate the possibility of litigation, that does not impose a companywide "duty to preserve." *Id.* at 217.

How then is a company to act in the face of threatened litigation? The answer from the case law is that parties must act reasonably. But what does that mean in practice? A company has three options when litigation is threatened: Suspend all backup tape rotation and preserve all data in the company; temporarily suspend backup tape rotation and begin a careful analysis to determine where relevant records might reside to see if the company can resume the rotation of tapes that contain information not relevant to the litigation; or continue normal backup tape rotation but immediately investigate who the key players are, interview them and the company's information technology staff, and promptly preserve any tapes identified as containing potentially relevant records.

While the "freeze everything" choice is obviously the most conservative and the one least likely to result in a spoliation claim down the road, it also has the most impact on the day-to-day operations of the company -- from both a business disruption as well as a financial perspective. Indeed, this approach could result in a considerable financial burden in a situation where litigation may reasonably be anticipated, but not actually filed for years. Is it fiscally responsible to preserve all data and suspend all backup tape rotation based on the

mere threat of litigation? In situations such as that, the third option -- continuing backup tape rotation along with immediate investigation -- is a balance of sound business judgment, fiscal responsibility and compliance with legal obligations.

Even with option 3, there are some potential pitfalls to watch out for. In *Zubulake IV*, for example, Scheindlin noted that, as a general rule, the duty to preserve does not apply to backup tapes used for disaster recovery purposes only. However, the court went on to identify an exception when a company can identify backup tapes containing data from "key players," which should be preserved in the face of pending or threatened litigation. *Id.* at 218. In the normal sequence of events, a company need not identify key players under Fed. R. Civ. P. 26(a)(1)(A) until approximately three to four months after the complaint is filed. By initiating the investigation as soon as the company "reasonably anticipates" litigation and preserving only those backup tapes that contain data from key players or relevant data not found on any active system, the company balances the need to comply with discovery requirements with its obligation to conduct business in a fiscally responsible way.

### INITIAL LITIGATION HOLDS

In *Zubulake IV*, the court also noted that once a litigation hold is in place, a party and its counsel must make certain that all sources of potentially relevant information are identified and placed on hold. Implicit in that statement is the mandate that the party needs to do the best it prudently and reasonably can under the circumstances. The litigation hold notice must contain sufficient detail so that the recipients can easily understand the categories of records that are relevant to the litigation and subject to preservation.

But, as discussed above, it may be very difficult for a company that "reasonably anticipates" litigation to act immediately with such specificity. What the company can and should do under these circumstances is to implement an initial litigation hold that is broadly disseminated within the company and describes as specifically as possible the types of records that need to be preserved. The initial litigation hold notice should also indicate that the litigation process is in its earliest stages and that more specific information will be forthcoming. The notice should also advise employees to notify a designated contact person if they become aware of any situation where relevant records are lost or destroyed.

Record retention/destruction policies can help a company that is facing litigation. Such policies govern both "retention" and "destruction" -- their purpose is to maintain business -- critical information and to destroy that which is not-and can help the company successfully defend itself in future litigation.

While there is no bulletproof approach for every company to follow in designing and implementing a well-reasoned and legally defensible record-retention/destruction policy and litigation hold once faced with litigation, there are some guideposts. Companies should be proactive and prepare, well in advance of litigation, a record-retention policy that is flexible enough to allow for the swift implementation of a litigation hold to preserve potentially

relevant records. Companies should also institute a regular review of the litigation hold to allow for adjustments as more information becomes available.

### Legal Interoperability

In cross-border use cases of EHR implementations, the additional issue of legal interoperability arises. Different countries may have diverging legal requirements for the content or usage of electronic health records, which can require radical changes of the technical makeup of the EHR implementation in question, (especially when fundamental legal incompatibilities are involved). Exploring these issues is therefore often necessary when implementing cross-border EHR solutions.

### Customization

Each healthcare environment functions differently, often in significant ways. It is difficult to create a "one-size-fits-all" EHR system.

An ideal EHR system will have record standardization but interfaces that can be customized to each provider environment. Modularity in an EHR system facilitates this. Many EHR companies employ vendors to provide customization.

This customization can often be done so that a physician's input interface closely mimics previously utilized paper forms.

At the same time they reported negative effects in communication, increased overtime, and missing records when a non-customized EMR system was utilized. Customizing the software when it is released yields the highest benefits because it is adapted for the users and tailored to workflows specific to the institution.

Customization can have its disadvantages. There is higher costs involved to implementation of a customized system initially. More time must be spent by both the implementation team and the healthcare provider to understand the workflow needs.

Development and maintenance of these interfaces and customizations can also lead to higher software implementation and maintenance costs.

### Regulatory compliance

- [Consumer Credit Act 2006](#) ?
- [HIPAA](#)

- [Health Level 7](#)

## Other EHR Sources of Information

- [Continuity of Care Record](#)
- [DICOM](#)
- [Electronic medical record](#)
- [European Institute for Health Records](#) (EuroRec)
- [Health informatics](#)
- [Health information management](#)
- [EN 13606](#)
- [MUMPS](#)
- [openEHR](#)
- [Personal health record](#)
- [List of open source healthcare software](#)
- [Health information exchange](#)

## References

1. [^ Gunter, T.D. and Terry, N.P. 2005 The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions in \*J Med Internet Res\* 7\(1\)](#)
2. [^ Electronic Health Records Overview](#)
3. [^ HIMSS - Electronic Health Record \(EHR\)](#)
4. [^ a b c Hillestad, Richard et al.: "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs", \*Health Affairs\*, 2005 \[1\], Retrieved February 19, 2008](#)
5. [^ .Hillestad, Richard et al.: "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs", \*Health Affairs\*, 2005 \[2\], Retrieved February 19, 2008](#)
6. [^ Hoffman S, Podgurski, A \(Fall 2008\). "Finding a Cure; The Case for Regulation and Oversight of Electronic Health Record Systems" \(PDF\). \*Harvard Journal of Law & Technology\* \*\*22\*\* \(1\): 107. <http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech103.pdf>.](#)
7. [^ Moore, Pamela \(2008\). "Navigating The Tech Maze". \*Physicians Practice\*. <http://www.physicianspractice.com/index/fuseaction/articles.details/articleID/1214/page/1.htm>. Retrieved 2009-08-23.](#)
8. [^ Gabriel, Barbara \(2008\). "Do EMRs Make You a Better Doctor?". \*Physicians Practice\*.](#)

- <http://www.physicianspractice.com/index/fuseaction/articles.details/articleID/1203/page/1.htm>. Retrieved 2009-08-23.
9. [^](#) [Electronic health records not a panacea](#)
  10. [^](#) Silverstein, Scot (2009). "2009 a pivotal year in healthcare IT". Drexel University. <http://www.ischool.drexel.edu/faculty/ssilverstein/failurecases/?loc=cases&sloc=2009>. Retrieved 2010-01-05.
  11. [^](#) Greenhalgh T, Potts HWW, Wong G, Bark P, Swinglehurst D (2009). Tensions and paradoxes in electronic patient record research: A systematic literature review using the meta-narrative method. *Milbank Quarterly*, 87(4), 729-88 ([full text](#))
  12. [^](#) Himmelstein DU, Wright A, Woolhandler S (2009). Hospital Computing and the Costs and Quality of Care: A National Study. *American Journal of Medicine*, doi:10.1016/j.amjmed.2009.09.004 ([full text](#))
  13. [^](#) [a](#) [b](#) RWIF, GWUMC, and IHP Staff: "Health Information Technology in the United States: The Information Base for Progress", Robert Wood Johnson Foundation, George Washington University Medical Center, and Institute for Health Policy, 2006 [\[3\]](#), Retrieved February 17, 2008
  14. [^](#) [Evidence on the costs and benefits of health information technology](#). Congressional Budget Office, May 2008.
  15. [^](#) DJ Ringold, JP Santell, and PJ Schneider; S; S (1 October 2000). "[ASHP national survey of pharmacy practice in acute care settings: dispensing and administration—1999](#)". *American Journal of Health-System Pharmacy* **57** (19): 1759–75. PMID 11030028. <http://www.ajhp.org/cgi/content/abstract/57/19/1759>.
  16. [^](#) Johnston, Douglas, et al. "The Value of Computerize Provider Order Entry in Ambulatory Settings: Executive Preview." Wellesley, MA: Center for Information Technology Leadership, 2003
  17. [^](#) Linder JA, Ma J, Bates DW, Middleton B, Stafford RS (July 2007). "[Electronic health record use and the quality of ambulatory care in the United States](#)". *Arch. Intern. Med.* **167** (13): 1400–5. doi:10.1001/archinte.167.13.1400. PMID 17620534. <http://archinte.ama-assn.org/cgi/content/short/167/13/1400>.
  18. [^](#) [a](#) [b](#) National Center for Health Statistics: [Electronic Medical Record Use by Office-Based Physicians: United States, 2005](#) Retrieved July 24, 2006
  19. [^](#) CDC's National Center for Health Statistics: [More Physicians Using Electrical Medical Records](#) Retrieved July 27, 2006
  20. [^](#) Raymond, B. and C. Dold (2002). "[Clinical Information Systems: Achieving the Vision](#)". Kaiser Permanente Institute for Health Policy. <http://www.informatics-review.com/thoughts/vision.html>.
  21. [^](#) Simon SR, Kaushal R, Cleary PD, et al. (2007). "[Correlates of electronic health record adoption in office practices: a statewide survey](#)". *J Am Med Inform Assoc* **14** (1): 110–7. doi:10.1197/jamia.M2187. PMID 17068351.
  22. [^](#) Menachemi N, Perkins RM, van Durme DJ, Brooks RG (2006). "[Examining the adoption of electronic health records and personal digital assistants by family physicians in Florida](#)". *Inform Prim Care* **14** (1): 1–9. PMID 16848961. <http://openurl.ingenta.com/content/nlm?genre=article&issn=1476-0320&volume=14&issue=1&spage=1&auiast=Menachemi>.

23. [^ http://recovery.gov](http://recovery.gov)
24. [^ http://healthit.hhs.gov/portal/server.pt?open=512&objID=1325&parentname=CommunityPage&parentid=21&mode=2&in\\_hi\\_userid=10741&cached=true](http://healthit.hhs.gov/portal/server.pt?open=512&objID=1325&parentname=CommunityPage&parentid=21&mode=2&in_hi_userid=10741&cached=true)
25. [^ Medical Records Institute](#), Retrieved December 6, 2006
26. [^ "We've got to adopt health information technology, and get on with it". \*Healthcare IT News\*. 2006-10-11. <http://www.healthcareitnews.com/news/weve-got-adopt-health-information-technology-and-get-it>.](#)
27. [^ "CEO Survival Guide to Electronic Health Records" \(PDF\)](#). National Committee for Quality Health Care. 2006. <http://www.nqfexecutiveinstitute.org/executiveinstitute/EHRbookfinal.pdf>.
28. [^ Columbus, Suzanne. \(May 2006\). "Small Practice, Big Decision: Selecting an EHR System for Small Physician Practices". \*Journal of AHIMA\* 77, no.5 \(May2006\):4246. \[http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\\_031357.hcsp?dDocName=bok1\\\_031357\]\(http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\_031357.hcsp?dDocName=bok1\_031357\).](#)
29. [^ "Towards the Electronic Patient Record: Ambulatory Market Trends: Discussion and Analysis" \(PDF\)](#). AC Group (Presentation). [http://www.acgroup.org/images/2007\\_TEPR\\_Meeting\\_-\\_Ambulatory\\_Care\\_Market\\_Trends\\_v2.pdf](http://www.acgroup.org/images/2007_TEPR_Meeting_-_Ambulatory_Care_Market_Trends_v2.pdf).
30. [^ "An Evaluation of Vista-Office EHR in the Small Practice Setting: Functional Performance, Economic Costs, and Implementation/Support Processes" \(PDF\)](#). Sujansky & Associates, LLC. [http://www.sujansky.com/docs/VistaOfficeEHR\\_EvaluationReport\\_2006-11-30.pdf](http://www.sujansky.com/docs/VistaOfficeEHR_EvaluationReport_2006-11-30.pdf).
31. [^ "The Value of Electronic Health Records in Solo or Small Group Practices". The Commonwealth Fund. \[http://www.cmwf.org/publications/publications\\\_show.htm?doc\\\_id=296446\]\(http://www.cmwf.org/publications/publications\_show.htm?doc\_id=296446\).](#)
32. [^ "Potential Benefits of Electronic Medical Records" \(PDF\)](#). LBJ School of Public Affairs. <http://www.wcit2006.org/Healthcare/media/whitepaper/emr.pdf>. Retrieved 2007-07-10.
33. [^ Meinert, D.B. \(2006\). "Resistance to Electronic Medical Records \(EMRs\): A Barrier to Improved Quality of Care" \(PDF\). \*Issues in Informing Science and Information Technology\*. <http://proceedings.informingscience.org/InSITE2005/I41f100Mein.pdf>.](#)
34. [^ \[http://www.himss.org/content/files/vantagepoint/pdf/vantagepoint\\\_0405.pdf\]\(http://www.himss.org/content/files/vantagepoint/pdf/vantagepoint\_0405.pdf\)](#)
35. [^ "A State Policy Approach: Promoting Health Information Technology in California". California Legislative Analyst Office. February 2007. \[http://www.lao.ca.gov/2007/health\\\_info\\\_tech/health\\\_info\\\_tech\\\_021307.aspx\]\(http://www.lao.ca.gov/2007/health\_info\_tech/health\_info\_tech\_021307.aspx\).](#)
36. [^ Parish, Colin \(March 20, 2006\). Edging towards a brave new IT world. \*Nursing Standard\* 27:15-16](#)
37. [^ <sup>a</sup> <sup>b</sup> <http://www1.va.gov/vadodhealthitsharing/page.cfm?pg=23> Retrieved March 4, 2010](#)
38. [^ <http://www1.va.gov/vadodhealthitsharing/page.cfm?pg=9> Retrieved March 4, 2010](#)
39. [^ <http://www1.va.gov/vadodhealthitsharing/page.cfm?pg=4> Retrieved March 4, 2010](#)
40. [^ Traynor, Kate \(2008\) National health information network passes live test. \*American Journal of Health-System Pharmacy\* 65.22: 2086-2087](#)

41. <http://gcn.com/microsites/2009-health-technology-solutions/federal-health-information-exchange.aspx> Retrieved March 4, 2010
42. <http://www.connectopenresource.org/about/what-is-CONNECT> Retrieved March 4, 2010
43. <http://connectopenresource.osuosl.org/sites/connectopenresource.osuosl.org/files/CONNECTOverview.pdf> Retrieved March 4, 2010
44. [NHS Connecting for Health: Delivering the National Programme for IT](#) Retrieved August 4, 2006
45. [Ian Quinn, "Electronic records are less efficient than paper, finds DH research lead"](#)
46. [Mason, Moya K. \(2005\). \*What Can We Learn from the Rest of the World? A Look at International Electronic Health Record Best Practices.\* <http://www.moyak.com/papers/best-practices-ehr.html>.](#)
47. [Mandl KD, Szolovits P, Kohane IS \(February 2001\). "Public standards and patients' control: how to keep electronic medical records accessible but private". \*BMJ\* 322 \(7281\): 283–7. doi:10.1136/bmj.322.7281.283. PMID 11157533. PMC 1119527. <http://bmj.com/cgi/pmidlookup?view=long&pmid=11157533>.](#)
48. [Ruotsalainen P, Manning B \(2007\). "A notary archive model for secure preservation and distribution of electrically signed patient documents". \*Int J Med Inform\* 76 \(5-6\): 449–53. doi:10.1016/j.ijmedinf.2006.09.011. PMID 17118701.](#)
49. [Olhede T, Peterson HE \(2000\). "Archiving of care related information in XML-format". \*Stud Health Technol Inform\* 77: 642–6. PMID 11187632.](#)
50. ["Integrating the New York citywide immunization registry and the childhood blood lead registry". \*Journal of Public Health Management and Practice\*: S72–80. 2004. The Master Child Index consolidated 4,610,585 records that were contained in both databases into 2,977,290 records through a match and merge system.](#)
51. ["Quality improvements in pediatric well care with an electronic record". \*Proc AMIA Symp\*: 209–13. 2001.](#)
52. ["Perspectives on integrated child health information systems: Parents, providers, and public health". \*Journal of Public Health Management Practice\*: S57–S60. 2004.](#)
53. ["Opposition calls for rethink on data storage". e-Health Insider \(UK\). December 2007. \[http://www.e-health-insider.com/news/3343/opposition\\\_calls\\\_for\\\_rethink\\\_on\\\_data\\\_storage\]\(http://www.e-health-insider.com/news/3343/opposition\_calls\_for\_rethink\_on\_data\_storage\).](#)
54. ["German doctors say no to centrally stored patient records". e-Health Insider \(UK\). January 2008. \[http://www.e-health-insider.com/news/3384/german\\\_doctors\\\_say\\\_no\\\_to\\\_centrally\\\_stored\\\_patient\\\_records\]\(http://www.e-health-insider.com/news/3384/german\_doctors\_say\_no\_to\_centrally\_stored\_patient\_records\).](#)
55. [Health & Medicine \(2006-06-26\). "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded." Los Angeles Times. <http://www.latimes.com/features/health/medicine/la-he-privacy26jun26,1,3180537.column?ctrack=1&cset=true>. Retrieved 2006-08-08.](#)
56. [CNN.com \(May 23, 2006\): \[FBI seeks stolen personal data on 26 million vets\]\(#\) Retrieved July 30, 2006](#)
57. [European Parliament and Council \(24 October 1995\): \[EU Directive 95/46/EC - The Data Protection Directive\]\(#\) Retrieved July 30, 2006](#)

58. <sup>^</sup> ["Personal Information Protection and Electronic Documents Act - Implementation Schedule."](#) *Office of the Privacy Commissioner of Canada*. [April 1, 2004](#). Accessed [February 12, 2008](#) <[http://www.privcom.gc.ca/legislation/02\\_06\\_02a\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_02a_e.asp)>.
59. <sup>^</sup> <sup>[a](#)</sup> <sup>[b](#)</sup> Pear, Robert. "Warnings Over Privacy of U.S. Health Network." *New York Times*, February 18, 2007.
60. <sup>^</sup> JM Appel. Why shared medical database is wrong prescription. *Orlando Sentinel*, December 30, 2008. [http://www.orlandosentinel.com/news/opinion/views/orl-opappel3008dec30\\_0\\_4065787.story](http://www.orlandosentinel.com/news/opinion/views/orl-opappel3008dec30_0_4065787.story)
61. <sup>^</sup> <sup>[a](#)</sup> <sup>[b](#)</sup> Nulan C (2001). "HIPAA--a real world perspective". *Radiol Manage* **23** (2): 29–37; quiz 38–40. [PMID 11302064](#).
62. <sup>^</sup> [Theo Francis, Spread of records stirs fears of privacy erosion, The Wall Street Journal, December 28, 2006 \[4\]](#)
63. <sup>^</sup> ["Lawyers Per 100,000 Population 1980-2003"](#). Congressional Budget Office. <http://www.newsbatch.com/tort-lawyerinc.html>. Retrieved 2007-07-10.
64. <sup>^</sup> ["Tort reform"](#). News Batch. 2006-05. <http://www.newsbatch.com/tort.htm>.
65. <sup>^</sup> ["Bigger focus on compliance needed in EMR marketplace"](#). Health Imaging News. 2007-02-05. <http://www.healthimaging.com/content/view/5885/89/>.
66. <sup>^</sup> [Medical Manager History](#)
67. <sup>^</sup> Laura Dunlop (2007-04-06). ["Electronic Health Records: Interoperability Challenges and Patient's Right for Privacy"](#). *Shidler Journal of Computer and Technology* 3:16. <http://www.lctjournal.washington.edu/Vol3/a016Dunlop.html>.
68. <sup>^</sup> ["Newly Issued Final Rules under Stark and Anti-kickback Laws Permit Furnishing of Electronic Prescribing and Electronic Health Records Technology"](#). GKLaw. August 2006. [http://www.gklaw.com/publication.cfm?publication\\_id=525](http://www.gklaw.com/publication.cfm?publication_id=525).
69. <sup>^</sup> ["New Stark Law Exceptions and Anti-Kickback Safe Harbors For Electronic Prescribing and Electronic Health Records"](#). SSDlaw. August 2006. [http://www.ssd.com/publications/pub\\_detail.aspx?pubid=9675](http://www.ssd.com/publications/pub_detail.aspx?pubid=9675).
70. <sup>^</sup> European Patient Smart Open Services Work Plan: [epSOS: Legal and Regulatory Issues](#) Retrieved May 4, 2008
71. <sup>^</sup> Clayton L. Reynolds MD, FACP, FACPE (March 2006): [Paper on Concept Processing](#) Retrieved July 27, 2006
72. <sup>^</sup> Maekawa Y, Majima Y.; "Issues to be improved after introduction of a non-customized Electronic Medical Record system (EMR) in a Private General Hospital and efforts toward improvement"; *Studies in Health Technology and Informatics* 2006
73. <sup>^</sup> Tüttelmann F, Luetjens CM, Nieschlag E.; "Optimising workflow in andrology: a new electronic patient record and database"; *Asian Journal of Andrology* March 2006
74. <sup>^</sup> The Digital Office, September 2007, vol 2, no.9. HIMSS
75. <sup>^</sup> Gina Rollins."The Perils of Customization." *Journal of AHIMA* 77, no.6 (2006):24-28.

### [\[edit\]](#) External links

- [Can Electronic Health Record Systems Transform Health Care?](#)
- [Health Information Technology in the United States](#)

- [How to Enable Standard-Compliant Streaming of Images in Electronic Health Records](#) a white paper by [Aware Inc.](#)
- [Open-Source EHR Systems for Ambulatory Care: A Market Assessment](#)(California HealthCare Foundation, January 2008)
- [US Department of Health and Human Services \(HHS\), Office of the National Coordinator for Health Information Technology \(ONC\)](#)
- [US Department of Health and Human Services \(HHS\), Agency for Healthcare Research and Quality \(AHRQ\), National Resource Center for Health Information Technology](#)
- [ICMCC portal: EHR info and blogs](#)
- [Security Aspects in Electronic Personal Health Record: Data Access and Preservation](#) - a briefing paper at [Digital Preservation Europe](#)
- [Comprehensive list of Electronic Health Records](#)