Securing Protected Health Information

Introduction

There is a common saying in healthcare, "if it isn't charted it didn't happen." Although this serves numerous purposes, most healthcare workers will recognize immediately that thorough charting is important for three reasons. First, a complete medical history is invaluable for determining present problems. This medical history also gives clues to potential health problems in the future. Second, the chart is necessary for coordination of healthcare. The teams of healthcare workers that must cooperate to appropriately treat an individual rely on the health record for the majority of communication between disciplines. Some might argue that the third reason is most important. Documentation is the only protection against malpractice lawsuits. Regardless of purpose, these records must be created and appropriately managed.

All major medical institutions have transitioned from paper to electronic health records (EHR). The Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009 set standards and provides incentives for the utilization of certified EHR technology. The laws continue to push the blame for exposures to the medical provider. The Board of Directors and CFO's of health organizations must adopt a failsafe strategy for protecting EHR. Past laws like Sarbanes Oxley (SOX) put the CEO and CFO of the health organization in the position of criminal liability with prison terms of up to 10 years for malfeasance. The ESI legislation and Rule 26 now pull the Board of Directors and the IT Managers into this same criminal liability position. Executives in the health industry have not caught up with their criminal, legal and financial exposure. Healthcare, like it or not, is a political battlefield and health organizations need to perform total risk management analysis to establish how to store, transport and share medical health records. The balancing act of ease of sharing patient files between departments, practices, specialists and the government and ensuring security data is fraught with danger. A new modality of protection similar to financial institutions or intelligence

agencies needs to be adopted by the medical records community.

Length of Retention

Every piece of current information is important. The question then becomes, how long should records be kept? Lack of a consensus by the various regulating and professional organizations makes it impossible to provide a single answer to this question. HIPAA regulations require that records be kept for six years. This is typically sufficient for any malpractice consideration, since the likelihood of developing a complication greater than six years following a particular procedure is negligible. The ability to establish causality over this great a period of time is even less likely. However, the Physician Company, a medical malpractice insurer, recommends a minimum of ten years following the last visit. In California, that recommendation increases to twenty-five years following the last visit[1]. This means that the absolute number of years stored per patient could be many decades, depending on the length seen by a particular provider.

Legal counsel upon receipt of a legal action immediately places a legal hold on everything related to that case. From that moment the retention period is "infinite" until the case is resolved or settled. Then the hard part is that the defendant and the plaintiff each have 99 days to create a "Data Map" of where the relevant records are stored. With a hospital this could include x-rays, MRIs, CT scans and back-up tapes with the data that has the case files. Now consider all of the iPads, notebook computers and smart phones that doctors carry. These could all be subpoenaed. Failure to include everything on the "Data Map" could jeopardize the case. The most prepared party has a huge advantage. Doctors are playing in a new world. If everything is put on back-up tapes then the data map is much easier to present in discovery meetings.

Multiply decades of records by thousands or tens of thousands of patients and it is easy to see that the quantity of information is massive. Let us look at a specific example of just how much data needs to be stored for a single institution. In 2011 the Chief Information Officer of Beth Israel Deaconess Medical Center (BIDMC) estimated that the hospital produced twenty terabytes of data per year.

BIDMC requires that images be kept a minimum of 7 years, with textual information retained for 15 years. Thus, the estimated storage requirement using these figures is 148 terabytes[2]. For health management organizations, that may be consolidating the information from numerous such entities, these numbers may be significantly greater.

Durability

The length of time that files must be kept presents a problem. Paper files under appropriate conditions can last indefinitely. Sadly, the same cannot be said for ESI. Current estimates are that data on disk is consistently viable for five years. This five year life span is fairly reproducible although it does not take into account the possibility of power loss or cooling system failure. Either of these situations can significantly decrease fidelity of the information contained therein. Typically, if and when a drive goes bad all of the information it contained is lost.

Some tape manufacturers will claim that their tapes are resilient enough to survive thirty years. More conservative estimates would consider 10 years reasonable, with an increase in this time under proper conditions. It is important to consider that humidity and temperature can affect the longevity of data tape backup. These conditions should be kept to as close to 70° and 40% relative humidity as possible[7].

Tapes are also susceptible to magnetic sources. Tapes are affected in fields of 10 milligauss or more over time. Higher fields can have immediate affects. Computer systems and tape storage in hospitals should be protected in magnetically shielded rooms. While hospitals are extremely careful about preventing metal anywhere near their MRI units, they often fail to examine the effects these imaging devices might have on media stored near or moving by such systems. The FIRELOCK Vault is magnetically shielded and can be placed near the servers and drives to prevent media from moving around the hospital and possible risk exposure.

Total Cost of Ownership (TCO)

Although some will not even consider data tape[3] as a potential option, this storage medium, typically relegated to second, third or even fourth line security, has been demonstrated time and again as the most cost effective solution[4-6]. The TCO for data tape is

commonly recognized to be at most one fifth the cost of other data storage media. In point of fact, the TCO of data tape is typically less than the price of cooling and providing constant electricity to disk storage devices. The footprint required for the same storage quantity is also less for data tape. Cloud storage is considerably more costly, though the ease of use and lack of space requirement is appealing to some.

Electronic Security

EHR are an appetizing target for electronic theft or extortion. Most EHR is relatively poorly protected and extremely valuable. In accordance with the HITECH Act, the US Department of Health and Human Services (HHS) has been charged with publicly reporting incidents of unsecured patient information breaches.

A list of all incidents in which five hundred or greater patient files were compromised is posted on the HHS web site. Since September of 2009 there have been 59 instances of hacking that allowed close to two million patient files to be breached in the US and Puerto Rico. The majority of these times it is believed that nothing was changed or removed[8]. Had any of these organizations simply encrypted their information they could have avoided liability. Encrypting tapes is familiar ground with no loss of speed. Encryption in the Cloud or on the online disk to disk platform is slower, fraught with higher error rates and 10 times more expensive.

From a security stand point, no one has ever hacked a tape in storage. Data is typically encrypted before being encoded on the tape. The need to transmit information from one health organization to another makes encrypting more problematic. Each unit needs a key (a system to break the encryption) and this translating slows down delivery. The more keys you have out there, the slower your system and the more likely someone is to just steal the encryption key.

Some of the more inventive criminals have created programs to encrypt information and extort a fee for the decryption key. One of the most famous examples of this is the encryption of all of the patient records of the Miami Family Medical Center in Australia. The owners reported that no information was compromised and opted not to pay $4,000 for the key. They were able to recover seven of the

previous eight years from backup storage and reconstruct the rest from labs, referrals and other health services[9]. Certainly, the cost was much greater than the $4000 asked, but the integrity of the information was without question. The solution to this potential problem is quite simple: regularly scheduled offline data backup.

Physical Security

Good old fashioned theft must always be safeguarded against. Several methods can be employed to decrease the likelihood of theft. The first is to limit access to the room or facility in which the data is housed. The transport of data must also be safeguarded. Care must be exercised if any company is hired to provide this service. In 2011 the EHR of 4.9 million members of Tricare, the insurance company that manages all veterans and military personnel, were stolen while being transported in the car of a Science Applications International Corporation (SAIC) employee. Several class action lawsuits were filed asking for $4.9 billion in damages[10]. Housing the backup on-site in a secure room or vault with fire protection and magnetic shielding provides a simple solution for all of these possibilities.

Between 2004 and 2006 over four thousand fires that caused significant property damage were reported in US healthcare facilities[11]. Fire, smoke and water will cause irreparable damage to any data storage medium. The loss of power associated with a large fire is detrimental to disk storage devices. Smoke and contamination from a fire will shut down the servers and removing the drives is not an option. Back up tapes offer a fail-safe solution with a 30 year proven track record of recovery.

Recommendations

1. Utilize linear tape for data storage. Data tape has proven over decades of use to be cost effective, durable and secure.

2. Duplicate, triplicate or even quadruplicate your storage. Regardless of medium chosen some data will always be corrupted. Infallible systems have yet to be created. It is significantly less probable that exactly the same piece of information will be lost from all copies. Place these copies in different geographic locations, if

possible, to decrease chance of loss due to natural disaster.

3. Store and manage the data without using a third party vendor. In case of litigation the vendor cannot be blamed for inability to produce information at discovery. If a vendor is necessary be certain that they are properly vetted, and store the data safe, durable, climate controlled facility.

4. Do not use cloud storage. Decreasing access to data is the first step to decreasing any threat of loss or compromise. Cloud storage is unreliable in litigation as clear evidence that all information is present and unaltered is virtually impossible to provide. Proprietary server vaults on site at the health organization where all connections are hard wired and data leaving the server room is moved outside the protected chamber in an encrypted tape with multiple copies stored in separate locations is a superior strategy. Offsite storage companies who offer Class 125 Vaults for tape storage are available in many markets.

5. Encrypt all protected information. Losing data is undesirable and potentially costly. Do not compound this problem by allowing the information to be read by anyone willing to steal the EHR. Decreased litigation costs, decreased HIPAA fines and decreased public shame on the HHS web site are all good reasons for encryption.

6. Keep all stored data in an appropriate environment. For optimal electronic, spoilage and disaster protection a quality storage vault is absolutely necessary.

1. http://www.thedoctors.com/knowledgecenter/patientsafety/articles/con_id_001849 accessed 10/27/13
2. http://geekdoctor.blogspot.com/2011/04/cost-of-storing-patient-records.html accessed 10/27/13
3. http://www.examiner.com/article/cost-effective-data-storage-solutions accessed 10/27/13
4. http://www.datacenterknowledge.com/archives/2013/07/18/data-tape-dying-a-slow-death-or-already-dead/ accessed 10/27/13
5. http://www.oracle.com/us/corporate/analystreports/corporate/esg-nersc-case-study-202702.pdf accessed 10/27/13
6. http://www.infostor.com/backup-and_recovery/tape/10-reasons-tape-storage-is-better-than-disk.html accessed 10/27/13
7. http://searchdatabackup.techtarget.com/tip/How-to-estimate-the-lifespan-of-LTO-tapes accessed 10/27/13
8. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html accessed 10/29/13
9. https://ama.com.au/ausmed/node/4194 accessed 10/30/13
10. http://articles.washingtonpost.com/2011-11-24/politics/35283695_1_saic-personal-data-data-theft accessed 10/30/13
11. http://www.usfa.fema.gov/downloads/pdf/statistics/v9i4.pdf accessed 10/30/13

Kendall DW Morris, PharmD, PhD, CPE

Dr. Morris has provided numerous services to an assortment of companies, universities and professional organizations over his 22 years in medical science. He began by studying the molecular mechanism of intravenous anesthetics, publishing two first author papers on this topic. Most recently, he has taught Anatomy, Physiology, Pharmacology and Scientific Communication and Research to a variety of future healthcare professionals. Dr. Morris is a native Floridian and father of two extraordinary children, Jade and Beck Morris.