

PREVENTING MEDICAL IDENTITY THEFT

Imagine your personal medical information has been affected a security breach. Then imagine finding out that your personal information has been used by someone to obtain medical treatments and even prescription drugs. The gravity of this breach becomes even more serious when you receive an invoice for the treatment, or worse, find out medical information in your personal file has been changed. The worst news is that this type of identity theft is becoming more and more common. Consider the following well-publicized situations reported in the media:

- Boxes of patient records from a doctor's office are found in a garbage dumpster
- A person receiving treatment at a small hospital is handed the medical records belonging to two other people
- A large medical center faxes patient records to the wrong place
- Medical records are found blowing around the street after being placed in a recycling bin for pick up
- A healthcare employee's laptop containing patient's personal information is misplaced or lost

These kinds of breaches can lead to cases of medical identity theft, which has become a growing problem. The World Privacy Forum estimates the number of medical identity theft victims to be between 250,000 to 500,000 people each year.

"Medical identity theft is "the fastest-growing form of identity theft in America today," says Wellmark Blue Cross Blue Shield's James Quiggle, Director of Communications for the Coalition Against Insurance Fraud in Washington. According to a Harris poll, the numbers are even higher with approximately four per cent of American adults, or nine million people, believing that they or a member of their family have had confidential medical information lost or stolen.

In May 2009, a Canadian provincial database that was storing medical information was hit by a computer virus and over 11,000 people's medical information was compromised. The information included names, addresses, healthcare numbers, lab test results and diagnoses. This is just another example of how prevalent this type of criminal activity has become.

Medical identity theft is also a very dangerous issue. This type of theft can expose a person's sensitive personal information which can then be used by fraudsters to get medical treatments, benefits, prescription drugs and generally defraud the medical system. The victims, whose medical records have may have been altered through the fraud, may ultimately receive incorrect medical treatment. If the victims learn their records have been altered during their own personal medical emergency, these errors could lead to incorrect diagnoses to even death.

"There is no doubt that the cost of a medical security breach can be dire to both the victim and the medical institution," says Michael McLay, Chief Executive Officer of Shred-it, an international information security company with a large number of healthcare clients. "While healthcare organizations and insurance companies could lose significant dollars by providing services to someone who will never pay, there is a bigger threat to the victims of medical identity theft."

CASES OF MEDICAL IDENTITY THEFT ARE GROWING

Khaled El Emam, a University of Ottawa professor and the Canada Research Chair in Electronic Health Information, reports that there is no clear understanding of the real scope of this problem because so few cases of medical identity fraud ever make it to the courts. In the US, said Mr. El Emam, where the for-profit health-care system creates incentives for hospitals and insurance companies to root out identity theft, an estimated 15 per cent of claims are considered fraudulent.

While hard to quantify worldwide, the costs of security breaches in the medical community have medical, psychological and financial implications: the pain and frustration of the loss of privacy, the loss of time, money and, in extreme cases, health or even life:

- According to the World Privacy Forum, medical identity theft may leave a trail of falsified information in medical records that can plague victims' medical and financial lives for years.
 - Compared to financial identity theft, victims of medical identity theft do not have a clear pathway to resolve the problem due to a lack of enforceable rights, according to the World Privacy Forum.
 - The victims of medical identity theft and fraud may also suffer the full range of financial consequences, typical for other forms of identity fraud, such as receiving statements for the credit cards they have never applied for or finding that their health insurance is exhausted.

From the standpoint of medical institutions, the consequences of medical identity theft may be significant:

- Healthcare providers may have to carry the burden of heavy fines, legal expenses, bad publicity and reputation loss. According to Forrester Research Inc., in 2006 companies that experienced security breaches lost between one and 22 million dollars.
- The average cost of a security breach is estimated to be as high as \$197 per compromised record and \$6.3 million per incident, estimated the 2008 Healthcare Information and Management Systems Society Analytics Report in the US.

THE MECHANICS OF THE BREACH

So how do fraudsters commit medical identity theft? Medical institutions produce large volumes of paperwork. The moment a hospital admits a new patient, a medical record is initiated. Moving through different phases of the medical process, the record accumulates a multitude of details – from the patient's lifestyle to symptoms, test results, diagnoses, treatment plans, procedures, insurance and personal information. These files, often kept in paper-based form, may continue beyond the original medical institution, making their way to other hospitals and clinics, family practice offices, insurance companies and other organizations.

According to Tom Hunter, Account Manager and medical sector expert at Shred-it, healthcare facilities generate significant amounts of confidential information.

"Hospitals generate a massive volume of paper every day," says Hunter. When Hunter is working with a medical facility on their information security needs, he finds it most helpful

to walk the patient floors and see firsthand how confidential paper information is being generated and how it is being handled.

In a hospital, many people – from doctors to nurses to lab technicians and others – may have access to patients' confidential information. While most employees would never use this information for fraudulent purposes, some may, either exploiting it themselves or leaking it to other employees. Some may work in tandem with large-scale criminal groups.

"Ideally," says Hunter, "there should be a locked confidential paper waste receptacle at each nurses' station and this paper waste should be collected for secure destruction every day."

There are other items of confidential waste that should be dealt with securely as well, including the plastic hospital cards that each patient receives upon being admitted to the hospital, as well as plastic employee ID cards. According to Hunter, it is best that this kind of waste is managed by a secure outsourced third party.

Security breaches may also result from the negligence of healthcare employees. While stories about medical files being dumped into recycling dumpsters or garbage containers – and even posted on the Internet – may sound anecdotal, such incidents do happen. These kinds of security breaches are becoming more common all over the world.

As noted by Hunter: "Some healthcare facilities have their own in house document destruction facilities, but it is a big undertaking for them." In situations like these Hunter says that there may be times when the hospital can't keep up with its document destruction requirements, and this backlog could provide opportunities for fraudsters to get a hold of information.

Medical records also must be stored for a period of time – often for 10 years, increasing the chances for a breach. Regular paper records are often kept for 10 years, and if it's a teaching hospital, or concerns a pediatric patient, they may keep the records for 15 years or even longer, notes Hunter.

"Often, the very practices used by medical institutions to store and dispose of their medical documents create situations where these documents can be easily mishandled," explains Hunter. He notes the following examples as situations where security breaches could take place:

- Confidential documents left in recycling boxes or garbage bins
- Lack of training for staff on what patient information should be protected and securely destroyed
- Unsupervised medical files in file rooms, on desks and in door folders
- Lack of focus on document destruction due to budgetary concerns
- Unsupervised in house document destruction facilities

"The major issue is what process healthcare facilities use to dispose of their paper documents," he says. "The key question is: do they make sure these documents are fully and securely destroyed?"

MEDICAL IDENTITY THEFT TRENDS

While there is no all-encompassing research on this, here are some of the trends in medical identity theft that Shred-it experts have compiled:

Insider wrongdoing

The most common pattern in medical identity theft involves healthcare insiders. According to the Healthcare Information and Management Systems Society, about 23 per cent of all breaches that required notification since 2000 have been caused by an employee. Examples include a temporary clerk convicted of stealing the identities of elderly patients for personal gain in Philadelphia and a Louisiana emergency room clerk who deliberately leaked patients' personal data, including names, birthdates and Social Security numbers.ⁱ

Organized crime

The people who work within the healthcare sector may sell stolen medical identity data to organized crime groups. Gary Auer, a fraud investigator for Blue Cross and Blue Shield, reported that such groups may set up dummy corporations for short periods of time – up to six months – and bill insurance companies for expensive medical equipment, such as wheelchairs, walkers, canes and beds. Given that such claims need to be paid within 30 days, insurers don't have time to check the authenticity of every claim.

“Infusion fraud”

Infusion fraud can be viewed as a variation of organized crime that is particularly particularly prevalent at HIV/AIDS clinics in Miami. In this scheme, fraudsters are billing Medicare for phony treatments with costly intravenous drugs, usually for HIV/AIDS and cancer.ⁱⁱ

“Consensual medical identity theft”

In this form of medical identity theft, a person who has medical insurance coverage may “lend” his or her insurance card to help an uninsured friend or relative. Plan members may also be tricked or bribed into exchanging their ID information for cash or goods. For example, criminals may approach the elderly with an offer to buy them groceries if they will show them their Medicare cards. People may also agree to trade their medical identities as a way to receive money. The growing numbers of the uninsured in the US - currently 47 million - are making this problem worse.

Internet disclosure

Medical information may be erroneously posted on the Internet, which may or may not result in identity theft and fraud. One recent example occurred in 2007 when information on thousands of California hospital patients, including their names and addresses and the departments where they received medical care, was accessible on the Internet for more than three months.ⁱⁱⁱ

Stolen or lost laptops

There are a number of examples when the security of patient information is compromised as a result of the loss or theft of laptops and data drives.

COMMON DOCUMENT SECURITY MEASURES

In the US, most medical institutions are using some kind of document shredding process, with some using outsourced third parties and some using shredders. However, their level of security varies widely, based on several factors:

- How is the process organized? Is all paper waste fully destroyed on a regular basis?
- Are there any security gaps?
- Is this process consistently implemented throughout the organization?
- Are all managers and departments committed to its integrity?
- Are all employees trained in secure document storage and destruction protocols?

- What are employees' attitudes to, and culture around, managing the paper trail?

"The most secure organizations have a 'shred-all' policy that basically eliminates human error," says Hunter. "A 'shred-all' policy means that, at the end of each and every day, all waste goes directly into locked receptacles for shredding rather than into unsecured recycling blue bins. Staff education and cultural change around the issues of document security are other prerequisites of compliance."

"For medical institutions, an outsourced document destruction provider such as Shred-it is an insurance policy that is a far better investment than paying for legal expenses and the consequences of reputation loss, resulting from the inappropriate handling of medical information," says Hunter.

LEGISLATION PROTECTING MEDICAL INFORMATION

In the US, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires healthcare organizations to "maintain reasonable and appropriate, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information" which includes patient medical records, patient logs, health insurance, billing and other personally identifiable health information.

In Canada, information collected by health care organizations on individuals is protected by PIPEDA – the Personal Information Protection and Electronic Documents Act. This legislation governs the collection, use or disclosure of personal information and applies to healthcare facilities and practitioners.

In the UK, patients' confidential information is protected by the Data Protection Act of 1998.

THE SHRED-IT SOLUTION

Working with 1,500 hospitals and clinics worldwide, Shred-it understands the challenges of the medical system. Balancing the protection of patients' medical records with budgetary constraints and patient information accessibility in a hospital environment is no easy task.

There are certain simple steps hospitals can and should take to protect the security of their patients' information:

- They should correctly identify the unique security challenges in their organization. In the medical environment these challenges typically include managing insider access to sensitive patient information. This is particularly important given that medical identity theft is often committed by employees
- Physically securing data
 - In a busy hospital setting, where a few seconds may mean all the difference between life and death, the emphasis is typically placed on speed and ease of access to information rather than on information security. The challenges of making medical information secure, both in paper-based and in electronic form, are particularly critical in the context of large medical organizations. In these large organizations, identity theft is three times more likely to occur than at smaller institutions, according to the Healthcare Information and Management Systems Society.
 - Integrating and managing the emerging large-scale e-health applications
 - Getting sufficient funding for security management systems, as well as the commitment at the top management levels to support these systems

While there is no single solution, medical institutions should consider the following solution components:

- Analyzing possible security gaps in their organizations and working with security experts to assess existing security systems
- Having ongoing risk analysis processes
- Having stringent and enforceable policies regarding access to sensitive patient information, as well as the protocols for authorization and authentication of individuals accessing health information
- Having strategies for dealing with security incidents
- Effectively integrating electronic information systems with clinical and administrative workflows
- Making sure that medical documents that are no longer required to be kept on record are destroyed in a secure manner

Kevin Watson of East Lancashire Hospitals Trust began researching the companies specializing in the disposal of confidential documents, admitting that Shred-it attracted him by its transparent on site document destruction methodology, with Trust representatives being able to watch the destruction process and receive certificates of destruction at the end.

“We felt that the time we would save and the risks to information that we would negate would justify the cost of the service,” says Watson. He also recognizes the productivity benefits of the contract with Shred-it, which has freed up their laboratory staff “to do what they are paid to do – work in the laboratory.”

Adds Watson: “The corridors are tidier, there is no longer a fire risk from bags of waste and the confidential documents are securely stored prior to responsible disposal. We have peace of mind that all information has been destroyed before it leaves the site.”

The value Shred-it offers to its medical clients extends beyond the physical process of destroying documents. Working as a strategic partner, Shred-it help clients identify and proactively manage their unique security risks. It addresses the full spectrum of their operational, security and financial needs, developing – and executing – a strategy that is both effective and cost-efficient.

Among Shred-it’s document destruction solutions are:

- Working alongside hospital Privacy Officers and departments to come up with custom solutions to protect patients’ private information
- Sharing and employing best practices learned at other healthcare facilities
- Understanding the budgetary restraints that affect hospitals, and coming up with the most cost-effective solution possible
- Providing the highest level of security in document destruction processes
- Training and sharing with hospital staff the importance of secure document destruction techniques
- For institutions with in house shredders, providing support when this process gets backed up
- Providing pre-screened, bonded and insured customer service representatives
- Allowing healthcare staff to view the document destruction process, if necessary

HOW SHRED-IT HELPS THE US VETERANS' HOSPITAL ASSOCIATION

Shred-it's secure document destruction process and expertise in servicing healthcare facilities has received the support of Veterans' Hospital Association (VHA), an organization that works on behalf of its 1,400 member hospitals and 23,000 non-acute care providers in the US. Shred-it is recommended by the VHA to its members, as one of only two approved document destruction providers.

According to Chris Sands, Portfolio Executive at VHA Inc., the organization has a five-tiered selection process that it applies before endorsing the services of any supplier. Some of the criteria Shred-it has met includes:

- The ability to service VHA members nationwide through a national footprint
- Experienced management team in all key positions
- Demonstrated integrity in business dealings
- Commitment to customer service in anticipating and responding to customers
- Track record on delivering promises and treating employees, business partners and customers with fairness and respect
- Bringing new ideas to customers to improve operational and clinical performance

Says Chris: "Shred-it's customer service team is very attentive and the company is always willing to go the extra mile to serve our membership."

WORKING TOGETHER TO ELIMINATE MEDICAL IDENTITY THEFT

Secure document destruction saves costs, increases employee productivity and enhances the reputation of medical institutions. But it also does much more, protecting patients from the medical, financial and psychological consequences of privacy breaches and identity theft and fraud. Shred-it works together with its healthcare partners to make sure patients' confidential information is secure.

Shred-it contact information:

T: 1.800.69.SHRED (74733)

Website: shredit.com

i Hospitals often fail to notify patients of data breaches; Regulatory loopholes keep patients in the dark, report says, Jon Brodtkin, 11 April 2008, www.networkworld.com.

ii The Week in Healthcare, Halting medical fraud; New coalition aims to stop various insurance scams, Gregg Blesch, 30 June 2008, Modern Healthcare.

iii Metro, 6,000 UCSF patients' info lands on Internet; Medical center didn't inform them of breach for 6 months, Elizabeth Fernandez, Chronicle Staff Writer, 2 May 2008, The San Francisco Chronicle.