SECURING
THE FUTURE

In this Issue

Protecting Patient Privacy: Why the medical community needs to take greater precaution in keeping records secure

For patients, confidentiality isn't a privilege or a nice-to-have—it's a right. With medical records containing everything from medical history to financial reports to personal contact information, ensuring that documents are stored and disposed of securely is of the utmost importance, both ethically and legally. In Canada, information collected by healthcare organizations on individuals is protected by PIPEDA – the Personal Information Protection and Electronic Documents Act.

However, recent media reports have shown that patient record security needs to be improved. In June, about a dozen medical records were found left behind on the grounds of Victoria Hospital in London, Ontario. While these were eventually recovered, it is unknown how long they were left exposed, meaning that personal information remains at risk. A similar situation also occurred with 1,000 medical records in Regina, Saskatchewan.

These instances are becoming more and more common, leading to widespread feelings of concern. According to the Healthcare Information and Management Systems Society, breaches are three times more likely to happen in a larger organization than in a small office—a fact that threatens not only confidentiality, but also the integrity of the medical community.

Why do Medical Record Breaches Happen?

There are many causes of a potential confidentiality breach and plenty of opportunities for one to occur given the fact that hospitals generate massive volumes of paper every day. Among the causes are:

- Unsupervised access - Often unsupervised medical files are left in file rooms, on desks and in door folders.
- Lack of training - Staff are not trained on what patient information should be protected and securely destroyed.
- Lack of focus on the importance of document disposal - Some healthcare facilities have their own in-house document destruction facilities due to budgetary concerns or limited resources. 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.
- Internal fraud - 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 or leaking it to other employees.

In the recent Shred-it Information Security Tracker, responses from individuals working in the medical sector showed that:

- While 81 per cent of medical professionals are aware of their legal obligations regarding patient document security, 55 per cent claim that staff are only trained on proper protocol on an ad hoc basis.
- 29 per cent of managers in the medical community state they have no employee directly responsible for managing document security.
- 21 per cent of respondents have never conducted an information security audit, and 55 per cent do not offer secure document disposal facilities within their organizations.

What's the Solution for Preventing Breaches?

The main way to prevent breaches from happening is to make document security a priority. While budgetary constraints or lack of knowledge may be a contributing factor to these lapses, the repercussions that result from a data breach are too damaging to ignore. Other options to consider include:

- Restrict access to patient information to necessary personnel.
- Develop an effective training program to ensure that all staff are well informed on how to destroy documents and why this process is important.

- Provide a secure document disposal receptacle where required, such as at each nurse's station or inside main examining rooms.

- Effectively manage both electronic and paper-based administration within a clearly defined workflow.

- Implement stringent hiring procedures and conduct background checks to reduce the risk of internal fraud.

When it comes to disposing of documents, enacting a "shred all" policy can help ensure that unneeded papers are properly destroyed. Furthermore, Ontario's Privacy Commissioner has stated that provincial institutions are required to either properly archive or destroy personal documents, and that disposal must be done through a cross-cut shredding method.

Using the cross-cut method of shredding, Shred-it's procedures make it nearly impossible to piece together the information once it has been shredded. Furthermore, Shred-it also destroys hard drives, meaning that medical records that are stored electronically can also be erased safely and efficiently. Customers also have the option of watching the process from inside the truck, making sure it's secure.

Your Free Security Consultation

To conduct your own security self-assessment, Shred-it has developed an online survey to help businesses better understand security gaps on their website at the following link:
www.shredit.com/fraudprevention

To learn more about Shred-it services or to book your FREE security assessment, visit http://www.shredit.com/

You can also visit Shred-it on Facebook or follow us on Twitter at @Shredit_Intl.

About Shred-it

Shred-it is a world-leading information security company providing document destruction services that ensure the security and integrity of our customers' private information. The company operates 140 branches in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.