JATHEON

DATA | KNOWLEDGE | INSIGHT

CASE STUDY

HOT TOPIC ISSUES

DATA SECURITY AND SENSITIVE INFORMATION CHALLENGES IN HEALTH CARE ORGANISATIONS

Introduction

Many health organisations, such as hospitals and health authorities are under intense scrutiny when it comes to data security, due to the extremely sensitive nature of the information they handle.

A data security breach for a health organisation can potentially be extremely costly and distressing for the individuals whose information is affected. What is more distressing is the fact that it is an unnervingly common occurrence. It is in fact a global issue found in hospitals and health centers around the world on a regular basis.

The example of three cases of data security breaches involving healthcare information, shows the importance of data security for any organisation dealing with sensitive data:

Our first case took place in **Woodwinds Hospital Minneapolis,** where 200 copies of confidential patient files were removed from the premises, and the lawsuit that ensued.

Our second case study looks at the costly consequences of not having a good data compliance policy in place. The **Peterborough Regional Health Centre** admitted responsibility for a number of breaches that resulted in the files of 280 patients being wrongfully accessed.

Our third and final case looks at the repeated failings of the **National Health Service in the UK** who have an unfortunately long history of data security breaches and the doubt this casts on their future ability to continue handling patient information.

CASE STUDY ONE

WOODWINDS HOSPITAL BLOWN AWAY BY BREACH

The Breach

In 2010, a member of staff from Woodwinds Hospital, St Paul, Minneapolis, removed 200 copies of confidential patient files, keeping them at her home for months without the hospital being aware of what had happened. The reason for this is now the focus of a lawsuit between the staff member, Barbara Peterson, and the hospital. Peterson claims she was told to destroy emails and notes that could be potentially damaging to the hospital's reputation. The hospital denies this. Whatever the truth may be, a member of staff was still allowed to leave the premises with confidential information and the hospital didn't notice this for months. This confidential information should not have been able to be destroyed anyway, if the hospital had an appropriate email archiving facility in place.

Regulations

The 'Health Insurance Portability and Accountability Act' (HIPAA) is concerned with the security and privacy of personal health information. The Act outlines the regulations health organisations must follow in regards to peoples' private health information, how it should be stored,

secured, who can access it, and how it should be disposed of.

Access

Health care organisations should make it clear which employees or departments are allowed to have access to electronic health information. Access to this information should be restricted to employees that need to access it as a part of their day-to-day work.

HIPAA also states that health organisations should also have a data back-up and disaster recovery procedures in place. Under the state law of Minneapolis, destroying documents that could potentially be used in a court case is against the law.

eDiscovery

If files can be removed from an organisation's system, whether it is a health organisation or otherwise, it needs to seriously consider the repercussions of not having a proper data back-up in place. An eDiscovery request that can't be fulfilled, because a file was removed or deleted incorrectly, could spell serious trouble for a health institution.

Training

To comply with HIPAA, health institutions must show that they have an on-going training program in place to teach staff how to properly handle private health information. This clearly wasn't done at Woodwind.

Staff must be aware of what is appropriate when it comes to accessing private health information. It they are not trained, the liability will ultimately rest with the organisation.

The Consequences

Apart from the potential lawsuit that the hospital now faces, it could also suffer from a damaged reputation. People naturally assume that any information that they provide to a hospital or their local doctor's office is stored securely. If this trust is tarnished, it can color a patient's view of a medical organisation.

WHAT COULD HAVE BEEN DONE DIFFERENTLY?

By making sure that their handling of health information complied with HIPAA, this entire incident could have been avoided. If there was a proper data back-up policy in place, the loss of emails wouldn't have mattered as they would have been backed-up on an email archiving system.

A clear hospital policy on accessing data, such as who can access it and what physical security protects the data. Training staff in good data management and data security is something every health institution must do. How can an organisation expect employees to adhere to laws if they aren't made aware of them? This situation could have been avoided with three simple steps: complying with HIPAA, creating a thorough data compliance policy and installing an email archiving system.

NEXT: *A $7M lawsuit highlights the importance of a good data compliance policy.* →

JATHEON

DATA | KNOWLEDGE | INSIGHT

CASE STUDY

CASE STUDY TWO

A $7M LAWSUIT HIGHLIGHTS IMPORTANCE OF A GOOD DATA COMPLIANCE POLICY

The Breach

Peterborough Regional Health Centre, just outside Toronto in Canada, is being sued for over $7 million by patients who had their files wrongfully accessed.

The hospital admitted that 280 patient files had been breached, with seven employees fired as a result. The breach in question was not just a once-off case; it happened many different times in different ways.

The Cases

In one case, a member of staff, who is also a teacher at nearby Fleming College, accessed files and allowed them to be viewed by a classroom full of student nurses.

In an entirely separate case, a woman who was treated by the hospital and wished to have her identity kept anonymous, had her file, which contained her name among other information, wrongfully accessed.

The third case involved a woman who was also a student at Fleming College and knew many people who worked at the hospital. She also wanted to keep her identity anonymous but her file was also accessed when it should have been kept completely private.

The Law

Under the Personal Health Information Protection Act (PHIPA), a piece of legislation applicable in Ontario, a health information custodian must protect a person's private medical information against "theft, loss and unauthorised use or disclosure and to ensure that the records containing the information are protected against unauthorised copying, modification or disposal". The hospital acted correctly when it informed patients that their files had been accessed, as this is also part of PHIPA. The Act also states that any person who has their private health information breached "may commence a proceeding in the Superior Court of Justice for damages for actual harm that the person has suffered as a result of a contravention of this Act or its regulations".

The Consequences

Peterborough Regional Health Centre now faces a potential lawsuit that could cost the hospital over $7 million. If staff were aware of data compliance laws this situation may have been avoidable. You can't guarantee that people won't act inappropriately, but if you give them the information and the knowledge required to make the right decision, then you drastically decrease your chances of something like this ever happening to your medical institution.

WHAT COULD HAVE BEEN DONE DIFFERENTLY?

While the hospital acted correctly when it notified patients that their files had been inappropriately accessed, that did not change the fact that their files had been accessed in the first place. On many separate occasions, staff accessed patient files when they shouldn't have. They then either shared them or caused

CONTINUED:
PETERBOROUGH $7M LAWSUIT CASE STUDY

the patients distress as they feared their personal health information would be released when they specifically stated that they wanted it to remain private. The hospital released a statement saying, "PRHC has a zero tolerance policy with respect to inappropriate access of medical records. This standard is not negotiable. If a breach is detected it is carefully investigated. If confirmed, decisive action is taken."

Data Compliance Policy

Despite being well-intentioned in terms of data protection, it's clear the hospital's staff were completely unaware of the regulations involved with good information security. The fact that a member of staff so flagrantly brandished private medical records in a classroom shows that the hospital never made them aware of the law and that it also had no data compliance policy.

By creating a robust and clear data compliance policy for staff to follow, the hospital could have avoided repeated instances of data breaches. A data compliance policy, after it is created, must be updated to comply with any changes in the law. Staff must be made aware of it and reminded of its importance on a regular basis, particularly in a medical institution where security of private information is of paramount importance.

NEXT: *What NHS' past failings teach us for the future.* →

CASE STUDY THREE

NHS PAST FAILINGS TEACH US A LOT FOR THE FUTURE

The Breaches

The NHS has been at the center of a number of data breach scandals. Recently, subsidiaries of the NHS have been fined for loosing patient information, for data ending up in the wrong hands, for not encrypting or securing data. NHS employees have been found to be disregarding IT usage policies and hardware containing personal health information has been found improperly disposed of. These repeated failings have brought doubt over the agencies ability to effectively protect patients' sensitive information.

The Law - Data Protection Act

The Information Commissioner's Office, the body responsibility for issuing the NHS with these fines, upholds the 1998 Data Protection Act and insists that the NHS as a body handling and storing health information must, among other obligations:

- Only collect information needed for a specific purpose
- Keep the information secure
- Ensure it is relevant and up to date
- Allow the subject of the information to see it on request.

If a company or a body like the NHS handles personal information it is required to register as a data controller with the ICO. Failing to do so is a criminal offence.

CONTINUED:
WHAT NHS'S PAST FAILINGS TEACH US FOR THE FUTURE

Regulations - Audits

The Minister for Justice has plans to give the ICO the power to conduct compulsory data protection audits on the NHS and local government health bodies.

Previously the ICO has had the power to conduct an audit on any company but must obtain consent first. The ICO formally requested this power given the nature of the information being handled by these organisations.

The ICO has said local government and NHS bodies were found to be the most complained-about organisations in terms of compliance with the Data Protection Act. It is thought that making these audits compulsory will help identify the practices that threaten the security of personal data and prevent further breaches.

Conclusion

Personal health information is a very sensitive topic and the more security measures the public can see are in place, the more secure they can feel in a system.

Learning from your mistakes is the best practice going forward. It is also important to implement this best practice as early as possible in the information process and ensure compatibility from the beginning to reduce the need for regulatory intervention and the risk of costly lawsuits.

In the end, it all comes down to care – delivering the same care and protection to your data as you would your patients or clients. Building up patient trust and faith in your ability to deal with their information in a respectful manner.

WHAT COULD HAVE BEEN DONE DIFFERENTLY?

Forcing organisations into compliance may be one effective method of minimizing threats and identifying possible breaches but it may be more efficient to implement changes earlier in the information process.

If these organisations were to adopt better IT practices, there is a greater chance that the information breaches of the past will not be repeated. A secure information storage solution that stores data in an encrypted format would limit the accessibility of the information to outside sources and restrict access from within the organisation. An effective archive would allow the organisation to comply with the legislation in storing the information securely while ensuring it is readily available upon request.

How Email Archiving with Jatheon Can Help

An on-site email archive from Jatheon is a straightforward solution for any organisation to ensure maximum data security and compliance. Your email archive stores all your email communication in a secure archive which prevents the deletion or wrongful modification of data. This information can be easily retrieved and restored without any risk of corruption or loss.

Email archiving with Jatheon can help in maintaining a strong data security policy and ensure compliance with regulations leaving clients with the peace of mind that all their information is highly secure.

CASE STUDY

JATHEON
DATA | KNOWLEDGE | INSIGHT

CONTINUED:
WHAT NHS'S PAST FAILINGS TEACH US FOR THE FUTURE

Best Practice Guidelines for Health Care Organisations

Draw up a clear Data Protection Policy for your organisation

- Adopt the necessary technical and policy solutions that meet regulations
- Train and inform staff of Data Protection regulations and compliance
- Ensure staff understand Data Protection Policies
- Archive and back up data both on site and off site
- Encrypt sensitive data
- Implement a system that prevents wrongful destruction or modification of information
- Regularly review data protection policies and staff training
- Have a system of timely notification for data security breaches
- Work with Data Protection Authorities to ensure optimum compliance

ABOUT JATHEON

Founded in 2004, Jatheon Technologies Inc. designed the world's first non-intrusive network appliance.

Today, Jatheon continues to raise the bar throughout the industry with its latest enterprise grade cCore appliance line, and ergo, its powerful email archiving, indexing, retrieval and dynamic monitoring software solution.

Jatheon is headquartered in Toronto, Canada and serves clients worldwide through its network of global business partners.

For more information, please visit ***www.jatheon.com****.*

888.528.4366 888.JATHEON
www.jatheon.com