JATHEON

DATA | KNOWLEDGE | INSIGHT

CASE STUDY

PROTECTING DATA IN HEALTH CARE

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 losing patient information, for data ending up in the wrong hands, and 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 agency's 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.

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.

TURN THE PAGE TO READ

WHAT COULD HAVE BEEN DONE DIFFERENTLY?

CASE STUDY

PROTECTING DATA IN HEALTH CARE:
NHS PAST FAILINGS TEACH US A LOT FOR THE FUTURE

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 deletionor 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.

JATHEON
DATA | KNOWLEDGE | INSIGHT

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

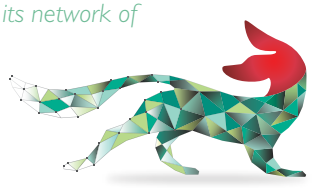
ABOUT JATHEON

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