

# The Health of IT Security

Laptop and mobile IT theft within  
the UK health sector

## Introduction

Laptops, netbooks and tablets have become an invaluable tool for those working within the health sector, enabling opportunities for remote working and greater flexibility. Although mobile IT devices bring considerable benefits to hospitals, trusts and other health authorities, the investment in valuable IT resources has resulted in the healthcare industry increasingly becoming the target for both organised and opportunistic theft.

This white paper examines the issues surrounding IT security within the UK health sector, including the problem of repeated laptop thefts, and offers practical advice for the industry's professionals to help them keep their mobile electronic devices safe.

## The symptoms

With a constant supply of accusatory news stories and 'shocking' statistics about laptop theft within the healthcare sector, it is understandable that some professionals experience information overload. Although simply spouting statistics will not make laptop theft disappear, examining data is important to put the industry's problem into context.

So, what are the facts?

- The NHS has been responsible for almost a third of all data security breaches reported to the Information Commissioner's Office (ICO) since 2007, according to research by IT consultancy Hytec.
- ICO data reveals that burglary and theft are the biggest security risks for organisations processing people's personal details.
- In a recent report by the Ponemon Institute, the health and pharmaceutical sector experienced the second highest rate of laptop loss than any other surveyed industry.

Laptop theft is clearly a very real and increasingly common issue for healthcare, but why should its professionals take IT security seriously?

## Cause for concern

Although a lost laptop causes inconvenience for its user, no matter what their job title, a laptop stolen from a healthcare worker can have far greater consequences.

According to the Billion Euro Lost Laptop Problem, from the Ponemon Institute, only two per cent of the cost of a lost laptop is due to actually replacing the device. In fact, a staggering 80 per cent of the cost ensuing from a stolen machine will be incurred as a result of data breaches. Crooks that steal laptops from the health sector often do so because the information stored on the machines is worth more than their resell value. If a laptop containing the sensitive information of patients, or confidential medical projects, falls into the wrong hands, patient safety could be severely compromised and clinical developments may be disrupted, not to mention the reputation of the organisation responsible. If stolen confidential data was passed on to blackmailers, the fall-out does not bear thinking about.

What is more, laptop theft can be incredibly costly. Amongst other components, when the financial impact of lost productivity, data breaches and forensics are taken into account, the Ponemon Institute estimates that the average cost of a missing laptop is a colossal €35,284. Moreover, not only will an authority have to source equipment to replace stolen laptops, but hospitals, trusts and other health organisations could face hefty fines. Since April 2010, the ICO has had the

authority to issue monetary penalties of up to £500,000 to those in serious breach of the Data Protection Act. As a result, the public purse may have to foot the bill for lapses in IT security at a time of economic hardship.

## Diagnosing the problem

With laptop theft entailing such dangerous consequences, just why is the phenomenon becoming so common within the health sector? With security blunders well publicised, is it that health professionals fail to take heed and implement preventative measures? Or is the problem due to a lack of clear guidance and anti-theft advice?

In the UK, the NHS complies with ISO/IEC 27002: 2005, a code of internationally-accepted standards of good practice for information security. These guidelines state that, not only should security be applied to off-site equipment, but that organisations should devise a mobile computing policy outlining requirements for physical protection of their electronic devices.

In order to comply with ISO/IEC 27002: 2005, and other regulations set out by the UK Government, the NHS has created an 'Information Governance Toolkit' that all staff are required to assess themselves against. The toolkit includes a 'Laptop Security Policy' containing the following advice:

- A Local Laptop Manager (LLM) should be appointed to take overall responsibility for the management of each NHS organisation's laptop estate.
- All laptops used for NHS business, or holding NHS information, should be uniquely identified and registered in the organisation's records as information governance security-relevant items.

*Hindsight is a wonderful thing. Although it may be easy to criticise the mistakes of others, it is essential that we learn from them to stop the small mistakes, with potentially devastating consequences, from happening time and time again.*

### Case Study: NHS North Central London

In June 2011, an unencrypted laptop, containing the details of more than 8 million patients, was reported lost or stolen from a storeroom at the London Health Programmes, part of NHS North Central London.

The laptop was one of 20 missing from the authority and contained details of cancer, HIV, mental illness and abortions that could be used by blackmailers. Although, reportedly, the data did not include patient names, it was feared that post-codes and information on gender, age and ethnic origins, that could potentially identify individuals, were also held on the laptop.

At the time of writing, the theft was believed to represent the largest ever data breach in NHS history.

Although NHS North Central London followed a procedure of deleting any sensitive electronic information once it had been processed, this policy was rendered useless because the laptop was taken before the data could be removed by staff. If the laptop was encrypted, the important data held on the machine would have been rendered largely useless to thieves. The Trust would have also been wise to invest in a purpose built cabinet constructed of reinforced steel to store their mobile IT in overnight, rather than locking them in a storeroom. Such cabinets are designed to resist crowbars and lock-picks and can also charge mobile IT devices if desired.

- The local IT Security Manager or equivalent should regularly review the NHS organisation's laptop estate to ensure that they continue to meet these requirements and that the residual level of risk from their use is acceptable.
- Laptops should be secured to a desk, or other appropriate point, if left unattended using an appropriate locking mechanism.
- When travelling and not in use, ensure that laptops are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Laptops left on display and unattended will inevitably attract attention and are likely to be stolen

Advice on IT security is also included within the 'Joint Guidance on Protecting Electronic Patient Information', compiled by the British Medical Association and NHS Connecting for Health. The guide states, "If you use a laptop or mobile device, you have a duty to ensure that you take appropriate precautions to protect the laptop and the data it contains. This includes reducing risk of theft by keeping the equipment out of sight and locked up whenever possible, using passwords and installing encryption software to protect sensitive data".

Although the above information is an excellent starting point, it contains relatively few practical tips explaining exactly how healthcare professionals can physically secure their laptops, netbooks and tablets. With demanding job roles and a focus on patient safety, healthcare professionals are, understandably, unlikely to have the time to seek out this step-by-step guidance if it is not readily provided for them. What is more, although NHS organisations are "recommended" to adopt the exemplar 'Laptop Security Policy' published by NHS Information Governance, this document does not appear to be compulsory to follow. Unfortunately, this ambiguity can risk staff viewing their compliance with this policy as optional. Although there are likely to be other factors, the absence of detailed practical advice for those working within the healthcare sector, and explicit rules for them to follow, is surely at least partly to blame for the recurrence of laptop theft.

### Case Study: Hull and East Yorkshire Hospitals NHS Trust

In November 2010, Hull and East Yorkshire Hospitals NHS Trust was forced to apologise after the data of more than 1,000 patients went missing from a doctor's home.

The incident occurred when a junior doctor acted outside of regulations in removing the unencrypted information and installing it onto his laptop, which was then stolen from his place of residence. The computer contained details of 1,147 individuals and listed their names, dates of birth, hospital numbers and treatments they had received.

Although the Trust wrote to each of the patients affected, the theft, understandably, upset local residents, promoting several angry outbursts in both the local and national press. One livid mother said: "I'm fuming about it. We should be able to trust these people." As a result, not only was patient safety compromised, but the reputation of Hull and East Yorkshire Hospitals NHS Trust was significantly damaged.

Although Hull and East Yorkshire Hospitals NHS Trust clearly had an IT security policy in place, the junior doctor responsible for the data loss acted in spite of these guidelines, suggesting that he was not aware of their existence. To prevent a similar problem in the future, frequent training should be given to all staff to ensure that they understand how to secure their mobile IT devices at work and when working remotely. A manager should also be appointed to make sure that this tuition is being given, and that the security policies are being followed.

## Treatment and prevention

It is, of course, unreasonable to claim that every instance of laptop theft could have been avoided, but cases could surely be mitigated if those that work within the health industry were provided with effective and targeted guidelines outlining exactly how they could physically secure their IT devices. In recognition of this problem, we have created some clear and simple security tips for healthcare professionals to keep their IT safe:

- Staff should take care to avoid accidentally advertising IT assets to thieves by refraining from discussing electronic devices on their organisation's website, social networking sites or informing the local press when a lot of new equipment has been purchased.
- When new equipment is bought, its packaging should be flattened, turned inside out and crushed before it is put outside with the rubbish, to avoid notifying potential thieves to a delivery.
- Laptops and netbooks should never be left unattended and should be secured to a desk using a lockdown system or fixed to furniture, such as a radiator, with security cables when in use. Security cables slot into a laptop's universal security slot and act as a deterrent against opportunistic theft by securing devices to any solid or fixed object. The cables are constructed of high-tensile steel and fitted with anti-drill locks to make it difficult for a thief to remove a laptop. Lightweight and portable, the cables are designed so that employees can carry them with them when working remotely or seeing client and are a must-have security device for professionals that are constantly on the move. Laptop lockdowns secure machines in a highly visible way for theft deterrent. The device can lock laptops to desks in the open position, enabling users to carry on working on the machines.
- Encryption software should always be installed onto mobile IT devices, even if the health authority it belongs to follows the policy of deleting information once it has been processed. If a thief steals a laptop before its contents can be destroyed, its information could still be accessed for illegal purposes. Encryption can protect patient records by scrambling data to make it difficult for unauthorised personnel to determine its meaning, often rendering it useless to thieves.
- Although encryption is vital to protect data, it should not be relied upon alone. Some thieves will not stop at anything, not least encryptions, to access important information, and those that steal laptops from the NHS often do so because the data that they contain far exceeds their resell value.

### Case Study: Calderdale Royal Hospital

In November 2010, a laptop containing details of around 1,500 people, was stolen from Calderdale Royal Hospital in Halifax. The laptop was part of a machine that scans skeletal muscles and held information that included names, dates of birth and addresses. The laptop went missing from a locked room, and was feared to be an 'inside-job'.

Again this fall-out from this incident could have been mitigated if the authority had simply encrypted their laptops. However, encryption should never be relied upon alone. As the theft may have been carried out by a member of staff, utilising physical restraints with Radio Frequency Identification (RFID) could have prevented the equipment from being removed, and would have made it much easier to identify the culprit and recover the item.

- Simply locking laptops in storage rooms will not keep them safe. Laptops and tablets are best protected in a secured lockable cabinet that can be bolted to the wall or floor. This cabinet should be constructed of reinforced steel, not wood or plastic, and be designed to resist crowbars, cutting equipment and lock-pickers.
- It should be compulsory for staff to follow laptop and mobile IT security measures by incorporating procedures, and penalties for breaching these procedures, into your company handbook and employee contracts. An IT security policy should be issued to all staff and employees should be made to sign this document to confirm their compliance.
- Staff need to be made fully aware of their duties regarding laptop security, and this includes regularly explaining relevant policies through company communication channels, such as emails and newsletters, and offering adequate training.
- External IT technicians should be made to present ID before they are taken to service computers and staff should ensure that they sign in and out.
- Ideally, laptops and other mobile devices should never be left unattended in a vehicle, unless they are stowed in a secure laptop car safe, because concealed areas like the boot or glove box will be the first places that thieves look. Laptops should never be left in a car overnight; it is far better to secure a laptop to furniture inside a building using a security cable.
- Laptop theft should be reported to the police as soon as possible; the quicker the police are aware that confidential information has gone missing, the more likely it is that equipment will be recovered and that health authorities will not have to seek a replacement.

In following the above guidelines, healthcare professionals can take easy steps towards preventing IT security breaches within their workplaces, especially if the advice forms the basis of a revised laptop security policy. All IT security procedures should be regularly reviewed and updated, and training should be provided to ensure that every member of staff understands how to prevent laptop theft and acts accordingly. A manager should also be appointed to make sure that this tuition is being given, and that the security policies are being followed.

## LapSafe® Products

LapSafe® Products is the UK's expert in IT security and the charging, tracking and management of various mobile electronic devices. With more than eleven years of experience within the public and commercial sectors, we created the UK's first laptop storage and charging trolley in 2000 and have lead the market ever since. We work alongside 500 of the world's biggest IT resellers and are dedicated to manufacturing technologically advanced, quality and value for money products that exceed the required safety standards.

For more information on IT security or laptop, netbook or tablet charging and management solutions, visit [www.lapsafe.com](http://www.lapsafe.com) or call free phone 0800 130 1456

## Conclusion

Laptop theft within the health sector can entail both dangerous and costly consequences, but its rise can be, at least partly, attributed to the lack of readily available practical advice regarding physical IT security. It is hoped that the suggestions documented in this white paper can go some way towards filling this void and help to mitigate future cases of theft of mobile IT devices in the NHS and wider healthcare industry.

## Appendix

The Health of IT Security whitepaper has been compiled using information from the following sources:

'Stolen laptop had details of 1,147 patients: Doctor faces hearing after theft from home', ThisisEastHullandRiding.co.uk, 18 January 2011

<http://www.thisishullandeastriding.co.uk/Undefined-Headline/story-11966234-detail/story.html>

'Missing: Laptop with 8.6million medical records', The Sun, 15 June 2011

<http://www.thesun.co.uk/sol/homepage/news/3637704/Missing-Laptop-with-86million-medical-records.html>

'Laptop theft leads to investigation at Calderdale & Huddersfield NHS', PublicTechnology.net, 3 February 2011

<http://www.publictechnology.net/sector/nhs-health/laptop-theft-leads-investigation-calderdale-huddersfield-nhs>

'A third of data security breaches down to burglary and theft', PublicTechnology.net, 13 November 2009

<http://www.publictechnology.net/content/21869>

'NHS on Amber alert', Risk-uk.com

<http://www.risk-uk.com/newsdetail.php?newsID=327>

The Billion Euro Lost Laptop Problem, The Ponemon Institute and Intel, April 2011

[http://antitheft.intel.com/Libraries/Documents/The\\_Billion\\_Euro\\_Lost\\_Laptop\\_Problem.sflb.ashx](http://antitheft.intel.com/Libraries/Documents/The_Billion_Euro_Lost_Laptop_Problem.sflb.ashx)

'ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management', iso27001security.com

<http://www.iso27001security.com/html/27002.html#Introduction>

'Laptop Security Policy', NHS Information Governance 'Joint Guidance on Protecting Electronic Patient Information', British Medical Association and NHS Connecting for Health

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/jointguidance.pdf>

## Resources

Readers of The Health of IT Security may also find the following articles helpful:

'Is your IT in safe hands?', Government Technology, July 2011

<http://www.governmenttechnology.co.uk/features2/item/2580-is-your-it-in-safe-hands>

'ICT Security Tips For Public Sector Professionals', Egovmonitor.com, 28 June 2011 <http://www.egovmonitor.com/node/42549>

'NHS should physically lock-down their laptops', PublicService.co.uk, 16 June 2011

[http://www.publicservice.co.uk/feature\\_story.asp?id=16782](http://www.publicservice.co.uk/feature_story.asp?id=16782)