Safe and sound: why a robust and workable data security policy is fundamental in healthcare programs

Dale Jessop

Exco InTouch, Unit 6, Wheatcroft Business Park, Landmere Lane, Nottingham, NG12 4DG, UK

Correspondence to: Dale Jessop. CTO, Exco InTouch, Unit 6, Wheatcroft Business Park, Landmere Lane, Nottingham, NG12 4DG, UK. Email: info@excointouch.com.

Author's introduction: Dale Jessop, Chief Technology Officer, leads the technology group at Exco InTouch and is responsible for directing the technology strategy of the business. As a software engineer himself, Dale is passionate about software development and has been involved with architecting a variety of systems since the late 1990s, including large scale programmes and national projects run by organisations such as the Audit Commission, the NHS Information Centre and Connecting for Health, as well as creating the architectural designs and strategy for high-volume transaction platforms.

Dale Jessop.

Received: 04 March 2016; Accepted: 08 April 2016; Published: 12 May 2016.

doi: 10.21037/mhealth.2016.04.04

View this article at: http://dx.doi.org/10.21037/mhealth.2016.04.04

There is no doubt that health and wellness data is becoming increasingly connected. Digital technology is now advancing at lightning pace and becoming more affordable, the cost of healthcare is rising and becoming a drain on national economies across the world. It is then obvious that healthcare organisations should adopt digital technology—however, with this new shift comes a whole host of security issues.

In the past, it has traditionally been financial institutions that have been on the receiving end of security breaches. However, in 2015, there was a new contender for the front pages; the health sector.

The year 2015 saw two huge hacks at health organisations. Excellus Blue Cross Blue Shield's security was compromised in August, with as many as 10 million people's name, date of birth, social security number, mailing address, telephone number, member identification number, financial account information and claims information compromised. Whilst

Excellus says it hasn't seen any misuse of the stolen data as yet, it's surely only a matter of time.

Even bigger than the Excellus breach was the one that occurred at Anthem in February of last year, which affected 78 million people.

The rise of security hacks in healthcare

Why do people want to steal the health records of others? Naturally, the first consideration is cold, hard cash. The FBI said recently criminals can sell healthcare information for as much as $50 a record. You only need to have a rudimentary grasp of mathematics to work out why they're so attractive.

Criminals have begun to move away from credit card fraud because the financial industry has finally put more robust security systems in place. What's more, healthcare data is much more comprehensive, and can be used for far more than just another line of credit; they can be used to secure anything from false healthcare insurance up to creating a completely false identity for someone.

According to a recent study by the Ponemon Institute (1), criminal attacks in healthcare are up 125% since 2010 and are now the leading cause of data breach. The findings also show that most healthcare organizations are still unprepared to address this rapidly changing cyber threat environment and lack the resources and processes to protect patient data. The same study showed that all healthcare organizations, regardless of size, are at risk for data breach and half of all healthcare organizations, both Covered Entities and Business Associates, have little or no confidence that they have the ability to detect all patient data loss or theft.

Understandably, this has huge implications for pharmaceutical companies seeking to provide digital health solutions. Reputation in the industry is everything, and the sector has notoriously had an uneasy relationship with the press over recent years—often being painted as the bad guys. If not even more important, however, is the impact on patient confidence and a potential knock on effect on health outcomes that any breach of security could bring.

Learning lessons from other industries

Healthcare and pharma companies should look to the financial industry for lessons on how to deal with data security issues. New technologies are either there now, or are very close to being in place whereby health records and wellness and fitness data is fully connected, and in the US possibly linking directly to your insurance premiums. There is also an emphasis on family members seeing some information on your health status or goals to provide motivation and support.

On a recent visit to the mHealth Summit in Washington DC, I noticed that the use of the word "patient" has begun to change to "person", so rather than being classed as a patient, pharma companies and healthcare organizations are seeing individuals as people in charge of their health rather than a patient being admitted or discharged and given advice.

With this in mind, plans must be put in place to ensure that systems are put in place to stop breaches of security. As ever, education is the key. Most breaches occur because hackers know something they shouldn't, and something as simple as malware sent via email can cause human error and a huge security lapse.

Pharma companies have to question themselves; do they have the right security checks in place to ensure the ever more sophisticated hackers cannot access the huge banks of data they hold; and very importantly do they have the relationships in place with organizations to help protect themselves by providing education, systems and training to combat the ever changing attack vectors?

Working together to create safer data

Every organization, regardless of their industry, needs a comprehensive strategy for protecting private data and responding to attacks. But a recent survey by Rand Secure Data discovered 44% of companies that responded have no formal data governance policy, and 22% have no plans to implement one.

Through ensuring separation of personally identifiable information (PII), the use of data encryption for locally stored data and program databases, and the inclusion of permissions for data handling in the ethics/IRB approved consent process, it is possible to build security and protection controls into software.

We have seen first-hand that more and more pharma companies are working with vendors who have taken these steps and incorporated them into the way they run their business. Working together to reduce the opportunity for human error through comprehensive education, and building all the necessary precautions into systems to encrypt data, but also determine suspicious activity in network and alert potential threats of attack.

It is now not a case of if, but when, digital healthcare will be introduced on a widespread basis throughout

the healthcare arena. It is the responsibility of everyone involved across the healthcare spectrum to ensure that data is as secure as it possibly can be, as by doing this we can maximise the potential for patients to remain engaged with the management of their health and ultimately improve health outcomes around the world.

Acknowledgements

None.

doi: 10.21037/mhealth.2016.04.04
Cite this article as: Jessop D. Safe and sound: why a robust and workable data security policy is fundamental in healthcare programs. mHealth 2016;2:19.

Footnote

Conflicts of Interest: The author has no conflicts of interest to declare.

References

1. Criminal attacks are now leading cause of data breach in healthcare, according to New Ponemon Study. Available online: http://www.ponemon.org/news-2/66