HealthManagement
Promoting Management and Leadership

Volume 14 - Issue 2, 2014 - IT Intelligence

IT Security and Privacy in Healthcare – The Need for Qualified Professionals

Author:

Tim Williams
International Healthcare Security and
Privacy Consultant & (ISC)2 Volunteer

Global Healthcare Trends

Delivery of healthcare is extremely reliant on skilled and motivated people. Patients' natural need for human contact means that people, not machines, will always play the primary role in healthcare. In countries with effective healthcare systems each person is likely to receive care from many healthcare professionals over the course of his or her life. Many healthcare staff may be involved, even in a single healthcare episode, and their need to access each patient's records means that if anyone ever breaches security or privacy, whether accidentally or intentionally, the consequences could be severe. Patient trust in healthcare organisations is highly dependent on everyone involved playing their part in protecting information.

There are many good reasons for increasing medical use of information technology (IT):

- Electronic records are simpler and quicker to access and cheaper to maintain than paper records;
- Electronic records can be richer and more useful than traditional records. For example, digital images can easily be enhanced and annotated. Video interviews and voice notes can capture information that historically would not have been retained;
- Machines can deliver more detailed, accurate and consistent measurements than people can;
- Automated monitoring systems can operate continuously day and night without breaks;
- Computers can assist skilled medical practitioners in different countries to collaborate and to build expert systems based on their combined knowledge and experience;
- Videoconferencing and telemetry can overcome the delays and costs of travel, putting patients in contact with medical experts more quickly and economically;
- IT can improve both the quality and the accessibility of medical training and continuous professional development.

However, increasing use of technology within healthcare means that information security and privacy arrangements effective when almost all medical records were kept secure using strong physical and personnel controls are no longer sufficient.

Other trends are also shaping the ways in which IT is being used within healthcare, for example:

- More data is being collected about each patient;
- Unit costs of electronic information storage and processing are falling;
- Medical records are being aggregated into ever larger databases to support epidemiological research;
- Medic al records are being accessed more frequently and by more people;
- The "Network Effect" is encouraging ever greater levels o f healthcare information sharing (Hillestad et al. 2005; Miller and Tucker 2009);
- Reduction of administration costs enables reallocation of funds to care delivery;
- The use of outsourcing to third party organisations is increasing, even in countries where most healthcare is provided by public institutions.

Healthcare is also becoming increasingly international. People travel more and require care outside their home country. Perhaps even more significantly, the sector attracts talent from around the world, creating a workforce that in most countries is highly internationalised.

Taken together, these changes are making it increasingly difficult to establish and sustain consistent security and privacy controls.

Growing Information Security and Privacy Risks

A significant barrier to ever-increasing medical exploitation of IT is that medical information security and privacy risks are growing in impact, frequency and variety.

There are frequent stories in the news about physical or electronic break-ins resulting in stolen data, or about mistakes, perhaps a significant data entry error or accidentally losing an electronic data storage device. Occasionally a medical device manufacturer reports a security or privacy vulnerability in a product that went through rigorous design and testing so would routinely be trusted. It is not uncommon to read of legal and regulatory fines and other penalties for data breaches.

Increasingly there are also news stories about:

- Risks associated with cloud computing that mean physical location of data is not controlled by the organisation and access to data is dependent on external networks also not controlled by the organisation;
- Risks associated with increasing use of personal computing devices such as smartphones and tablets, the so-called 'Bring Your Own Device' (BYOD) phenomenon;
- Risks that pseudo-anonymised medical records released to researchers may be linked with other information to re-identify individuals, invalidating assurances given to patients that their personal information is being safeguarded…and more.

Importance of Information Governance

Effective clinical risk management relies heavily upon effective information risk management. If information needed to support medical processes is not available or is inaccurate, there will inevitably be negative impacts on clinical outcomes.

In healthcare organisations that manage information risks effectively, delivery of positive clinical outcomes rests heavily on all aspects of information security, including:

- **Availability** - information needed to support clinical decisions is there when needed;
- **Integrity** - information needed to support clinical decisions is complete and accurate; and;
- **Confidentiality** - ensuring that sensitive personal details are handled appropriately.

Only by providing patients with robust assurances of sustainable privacy will the quantity and quality of complete and accurate healthcare information be maximised.

Establishing clear lines of accountability and responsibility for information risks is a growing priority at the organisational level. Within many organisations frontline staff feel unclear about who is responsible for which aspects of information risk. Because many partner organisations may be involved in delivering healthcare and many information exchanges occur between staff working for different organisations, it is frequently extremely difficult for people without specific competence in information risk management to determine:

- What security and privacy policies are applicable;
- Which country's laws have precedence;
- Who has primary responsibility for information security and privacy;
- What their own responsibilities are for supporting information security and privacy.

By nominating appropriately qualified and experienced individuals to perform information governance duties, usually alongside their primary role, management can do much to support their frontline staff and minimise uncertainty.

Embedding effective information security controls into clinical working practices across multiple organisations requires both an understanding of the prevailing culture and experience in establishing and sustaining an appropriate information governance regime. Broad consensus needs to be reached between all parties about:

- Which roles within which organisations have responsibility for which aspects of information security and privacy;
- Which stakeholders need to be consulted about changes to information security and privacy policies;
- Which stakeholders need to be informed (educated) about information security and privacy controls.

In any information governance negotiation involving multiple healthcare organisations, it is only possible to achieve broad consensus if a good proportion of the parties involved:

- Understand the unique challenges of the healthcare sector;
- Can effectively explain to their colleagues why information security and privacy matters;
- Are competent in the specifics of implementing information security and privacy controls within healthcare sector organisations.

Building Information Governance on a Firm Foundation of International Standards

One of the best ways to achieve the consensus required is to meet or exceed internationally recognised minimum standards. Implementing processes and controls that meet or exceed national standards may also be necessary, but organisations involved in any international activities need to identify common processes and controls which meet the needs of multiple countries.

When it comes to building effective information governance regimes and standards for healthcare organisations it has historically been difficult for managers to identify suitable international standards to build on, because many industry security and privacy standards have been:

- National and/or;
- Focused on particular technologies; and/or;
- Tightly controlled by proprietary commercial interests.

The (ISC)2 Healthcare Information Security and Privacy Credential

In recognition of the void in established international personnel standards the International Information Systems Security Certification Consortium, Inc (ISC)2®, best known for its cross-sector professional certifications in information security, pulled together a diverse team of subject matter experts from multiple countries to develop the Healthcare Certified Information Security and Privacy (HCISPP) certification.

The HCISPP sets a credible minimal international standard of knowledge and experience for anyone working in healthcare to whom management assign information security and/or information privacy responsibilities. The initial goal is to establish a broad base of competence spanning multiple countries and organisations. It is hoped that these HCISPP-certified individuals will in turn contribute significantly to the establishment of effective information governance arrangements in numerous healthcare organisations.

The HCISPP certification standard has intentionally been set at an accessible level that does not require degree-level education or prior experience in any specific medical or IT specialism. Nevertheless, even knowledgeable and experienced candidates will probably find t hat they need to study and learn new material in order to pass the exam, because of the diverse range of practice standards.

Candidates for certification must have healthcare sector work experience and have made an effort to study the specifics of information security and privacy in some depth and breadth. Good knowledge of just one country's laws and regulations is unlikely to be sufficient. Successful candidates will have needed to study a wide range of references and be aware of international differences in security and privacy laws and regulations.

Healthcare organisations can expect someone with the HCISPP certification to understand how information security directly impacts specific scenarios, for example:

- The timely availability of information about an individual's allergies is important to ensuring that no further exposure to the allergen occurs during treatment;
- The integrity of the information used to configure a radiotherapy machine determines whether many patients receive the correct dose - too much or too little radiation could be fatal;
- Preserving the confidentiality and privacy of the medical records of a victim of crime is essential to protect the victim from further harm from the perpetrator.

To reflect the breadth of perspectives required, HCISPP candidates are examined to ensure that they meet minimum standards of knowledge in six domains:

- Domain 1 - Healthcare Industry;
- Domain 2 – Regulatory Environment;
- Domain 3 - Privacy and Security in Healthcare;
- Domain 4 – Information Governance and Risk Management;
- Domain 5 - Information Risk Assessment;
- Domain 6 - Third Party Risk Management.

The HCISPP Candidate Information Bulletin is a good resource, even for those who do not wish to take the HCISPP certification examination, for understanding more about these topics or seeing the underlying references for the syllabus.

The core data security and privacy knowledge base will evolve and expand over time. However, healthcare organisations looking for confirmation that an individual is ready to start playing an active part in developing an effective information governance regime would be hard pressed to find better evidence than that they have studied for and attained the HCISPP certification.

Published on : Wed, 25 Jun 2014