HealthManagement
Promoting Management and Leadership

Volume 15, Issue 1, 2013 - Matrix

Data Privacy in a Wider Perspective of Risk Management

Data privacy awareness has increased significantly within the health sector over the last few years; this is mainly due to EU and national legislation. Another reason is the adoption of new technologies, such as the electronic patient file and electronic prescriptions. However, data privacy is not limited to Information Technology (IT); the physical protection of paper files, CD ROMs, USB sticks, etc. should be taken into account when tackling data privacy.

Data privacy should be seen in a wider perspective of risk management and governance. Due to recent events (e.g. the financial crisis), governance and risk management are hot topics for media coverage, especially within the financial sector. However these topics are also high on the agenda in the boardrooms of private companies in the corporate world, due to earlier scandals like Enron and Worldcom. Risk management is still in its infancy in healthcare, even though risks are probably highest, involving human life.

Responsibilities Regarding Risk Management

Regardless of the type of organisation, it is the responsibility of management to manage all risks of the organisation. This is also the case in healthcare and non-profit organisations. Besides, it is not only the responsibility of management to manage risk; it is also the responsibility of the board of directors to supervise whether risks are adequately managed within the organisation.

Worse: If risks are not adequately managed and events (accidents) occur, the directors can be held (legally) liable for this. This is not just theory, but happens in practice. Members of the board of directors often do not realise they are the final responsible and might be held liable in case of serious events. This is also apparent in healthcare, where directors are often appointed in an informal way and risks relate to human life.

Many risks, especially in healthcare, cannot be reduced to zero. Even when precautions are taken events could still occur. Precautions reduce the probability or the impact of a risk, however risks are often not completely eliminated. Therefore it is important, in case of such an event, to be able to prove that measures were taken to manage the risk and that the management has reflected and taken conscious decisions to manage the risk. Then, if it happens at least the management took all possible measures and cannot be accused of negligent omission.

Which Risks Should be Managed?

All risks of the organisation should be managed. There is a wide variety of risks, the most common categories are:

- Medical and patient safety risk;
- Operational risk;
- Legal & compliance risk;
- Financial risk; and
- IT risk.

Risks relate to all activities of the organisation, both at the care and at the administrative side. Within the above risk categories, there are many distinct risks that should be managed. For all important risks, control measures should be taken to prevent them from occurring and very often, IT plays an important role in this.

What Does it Mean to Manage Risks?

Proper risk management implies that:

- All important risks within the organisation are known and assessed, this is typically done in a risk assessment exercise;
- Based on the risk assessment, conscious decisions are taken to address the risks (or not!);
- Based on these decisions, appropriate actions are taken and measures are implemented to address the risks.

A risk assessment is typically performed with the aid of external consultants, preferably with experience in healthcare. The main reason for this is that many of the risks are generic and also present in similar organisations. A good consultant has a sectorspecific risk model to conduct the risk assessment. The risk assessment is typically performed in two phases:

1. Identification of all risks: This is typically done in workshops with management starting from the generic risk model;
2. Evaluation of all identified risks: There are several methodologies to evaluate risk; in practice both the probability and impact of the risk occurrence (the event) are evaluated.

The risk assessment exercise will provide you with an inventory of all risks and their evaluation. Of course, the highest risks will be addressed first.

In a next stage, decisions are taken on how to address the risks, based on their importance and possible measures. Basically, risks can be addressed in the following ways:

- Reduce the risk by implementing control measures;
- Delegate the risk, in practice this is most often done via insurance;
- Avoid the risk, for example by ending the related activities; and
- Accept the risk and take no action.

Indeed, the decision might be not to take any action. This might be because the risk is low and the cost is high. Most important is that these are conscious decisions, by management or even the board.

The decisions should also be documented, known and supported by all relevant people. Because, if 'an accident' happens, we want to avoid 'finger-pointing' and 'I thought you were taking care of this'. Based on the decisions made, an action plan is defined, which takes into account the priorities defined in the risk assessment.

What About IT Risks?

IT often plays an important role in management of many risks, especially operational and financial risks. On the other hand, there are also the specific IT risks. These are typically categorised with the acronym CIA:

- Confidentiality of information;
- Integrity of information; and
- Availability of information and systems.

Confidentiality of information is much related to data privacy. A commonly used definition of the confidentiality principle is: 'Only authorised people should have access to (view) confidential information'. Confidentiality risks are related to the abuse of the information. Typical control measures are related to the secure protection of confidential information.

Integrity of information is related to the correctness of the information. A common definition of the integrity principle is: "Only authorised people should have access to change information." Integrity risks are related to unauthorised changes to information. In healthcare these changes might ultimately lead to inappropriate medical decisions and actions, such as wrong medication. Therefore, integrity of information is probably even more important than confidentiality of information (data privacy) from a risk point of view. Fortunately, typical control measures are similar and also related to the secure protection of information.

A lot of information has been digitalised over the last years, and a lot of activities have been automated. New technologies have been adopted, such as the electronic patient file and electronic prescriptions. As a consequence, dependency on IT systems has increased tremendously in the last few years, hence the importance of systems availability. Needless to say, what the impact of unavailability of critical systems might be, fortunately also non-IT management easily relates to this, which facilitates decisions on investments to increase systems availability. Examples are systems redundancy, virtualisation of CPU and storage, Disaster Recovery Plans (DRP), etc.

Information Security: Burden or Need?

In many organisations during the last year the focus has been on systems availability and infrastructure. Less effort has been made on confidentiality and integrity of information. An important reason for this is that information security is not a popular subject and often associated with passwords. Endusers do not always see the benefits of this, especially not in highly operational environments, such as hospitals.

Therefore, it is important to find the equilibrium between operational efficiency and security. Identification via badges or biometrics (eg. finger prints) are examples of efficient and secure solutions.

Awareness creation on information security is not easy, the message should be: Not only, an unauthorised person would gain access to confidential information (infracting data privacy laws); not only, an unauthorised person would be able to modify critical information; but most important: people would believe it was YOU! Indeed, all actions performed on IT systems are logged nowadays. In case of malicious events, these logs are investigated and the events will be linked to you personally.

And, as earlier discussed, questions will probably also be raised towards management and the directors whether all precautions have been taken to prevent this from happening; and whether sufficient efforts were made towards information security.

An Action Plan Towards Information Security

We have seen that information security is an important element of risk management. Therefore it should be no surprise that the approach to address information security is similar to the approach on risk management.

In a first phase, a risk assessment is performed consisting of:

- Identification of critical information from confidentiality and integrity point of view, starting from an inventory of all systems and information;
- Evaluation of the identified critical information: The degree of criticality is determined based on the potential impact of confidentiality or integrity breach of the information.

Please note that the aspect of availability can easily be included in this exercise. It should also be noted that in similar organisations, critical information is also similar. In a next phase, an inventory is made of the information security measures already in place to protect the critical information. These measures include security procedures, access controls, passwords, security settings, access rights, etc.

Based on the criticality and security measures in place, it is determined whether additional measures should be taken. What is sufficient? This is

a difficult and subjective discussion. Most organisations refer to information security standards; the most common is the ISO27001 standard. However, this standard consists of 130 security controls to be put in place to comply with the standard. This is not feasible for most organisations.

So even when using standards, subjective decisions need to be taken on what is acceptable and not. These decisions should not be taken by the IT manager alone, other members of the management team and often even the Board should be involved.

Conclusion

Data privacy should be seen in a wider context of information security and risk management. Perfect security protection does not exist; risks can never be completely eliminated. Even in 'Mission Impossible', security was insufficient to keep the hero out of the computer.

The most important thing is that conscious decisions are taken, based on analysis and that these are formally documented and appropriate actions are taken. So that finally, liabilities are limited in case of events and no one should say "Ich habe es nicht gewüsst ."("I didn't know about it").

Author:

Koen Claessens
Director
BDO Risk & Assurance Services Burg
koen.claessens@bdo.be

Published on : Fri, 22 Mar 2013