Legal Information Management, 10 (2010), pp. 51–54

doi:10.1017/S1472669610000125

Getting the Right Balance: Information Security and Information Access

Abstract: This article by former law librarian, Jennifer Smith, highlights access and security issues to consider when handling sensitive information. Jennifer is a Director of the Information Management and IT consultancy, OneIS, which specialises in working with smaller organisations with complex information management requirements. The article provides practical advice and is particularly aimed at readers working in organisations without dedicated information security professionals.
Keywords: information security; SMEs

Introduction

> "The more secure you make something, the less secure it becomes. Why? Because when security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security. Hence the prevalence of doors propped open by bricks and wastebaskets, of passwords pasted on the fronts of monitors or hidden under the keyboard or in the drawer, of home keys hidden under the mat or above the doorframe or under fake rocks that can be purchased for this purpose".
>
> Don Norman, 2009[1]

The safest way to protect sensitive, personal or confidential information is to hide it away and never let it see the light of day, but information needs to be accessible to be useful. The best approach is to get the right balance between information security and access.

My company, OneIS, often works with organisations which need to share sensitive information amongst a dispersed team, and we provide an online information management system to enable this to happen. The hosting is completely under our control, is based in the UK, and with no part of the service outsourced to a third party. We tend to work with smaller organisations who want the benefits of using an internet-based solution, but with information too sensitive to entrust to the larger providers such as Google or Amazon.

But there is more to ensuring information security and information access than just choosing the right technology. As we work with smaller organisations without in-house IT or information management expertise, we are often required to provide extra assistance in ensuring that they have the right policies and are following best practices to keep their information secure and accessible to the right people at the right time. Because these organisations have limited resources, our solutions need to be practical and easy and quick to implement and maintain.

Whether you are responsible for the management of sensitive information or handle confidential information in the course of your work, almost everyone needs to be aware of good information security practices. This article provides a checklist of issues to consider when handling sensitive information based on our experience helping organisations get the right balance between information security and access.

1. Audit

It's important to begin with a clear idea of what information you have, what level of security it requires, and who needs to access it.

As an example, we have recently worked with a private medical practice:

i. What information do they have?

The main information held is patient records, which includes basic contact and demographic details about a patient, patient notes and files such as test results.

ii. What level of security does the information require?

This is highly sensitive personal information. It is critical that it is kept confidential for the well-being of the

patient; for protecting the patient-clinician relationship; for the reputation of the private medical practice and to avoid fines and penalties. The practice is bound by both UK law, particularly the Data Protection Act 1998, and regulations within the medical profession, particularly the General Medical Practice's confidentiality guidelines.

iii. Who needs to access the information?

Clinicians and associated healthcare practitioners need access, sometimes from outside the practice, as private healthcare practitioners frequently work in a variety of clinics and hospitals. They may require fast access to records to enable a quick response in patient care. Practice administrators will also need access for administration and billing.

Patients and regulatory bodies may request access. Although this is unlikely to happen frequently, it is important to respond promptly and provide comprehensive access when receiving such a request, so this scenario must be considered when planning access.

2. Planning

With a clearer picture of the information held, how sensitive it is, and who needs to access it, you can plan the security and access required. Having a good idea of the legal and regulatory requirements is crucial during this planning stage. Not only does it avoid your organisation failing those requirements, but it helps clarify the limits of your obligations so you do not impose unnecessary security restrictions which hinder effective business operations.

3. Policies and implementation

Effective measures require both policies and practical implementation. Most importantly, one person within the organisation should be nominated as having ongoing responsibility for overseeing information security.

i. Staff guidelines and training

Ideally information security should be considered throughout the staff recruitment process by checking references and qualifications, including obligations in employment contracts, and as part of induction training. All staff should be provided with written guidelines on how to handle information which helps ensure good practice, can help avoid security problems, and may provide your organisation with some defence in the event of a breach.

Staff guidelines should cover day-to-day business activities, including who to contact in the event of an incident and which other organisations may need to be informed after an incident. The Information Commissioner's Office (ICO) provides a library of good practice notes on its website which can help when producing staff guidelines.

All staff should receive training in information security. Carelessness and human error is as much, if not a greater, threat to data loss than technology. Training should include every way in which security could be breached e.g. overheard conversations; disposal of paper information or even sharing seemingly innocuous information on social networking sites.

ii. Technology

As virtually all information is processed using technology, the choice of IT systems is critical for ensuring information access and security. For smaller organisations with limited in-house IT support, a hosted internet-based IT system can be a good solution. With these types of services, the solution provider takes responsibility for storing the data securely, and users access it over the internet.

Organisations processing personal data are restricted under the eighth principle of the Data Protection Act as to the countries where that information can be processed. They must ensure the hosted solution provider will not transfer personal data beyond the countries allowed under the Act.

iii. IT security

Keeping confidential information secure is critical for businesses, and for organisations processing personal data it is a legal requirement under the seventh Data Protection Act principle. When using a hosted system, the solution provider will take care of the security of the information in the system, but it is still important to protect the security and integrity of computer hardware and other software used with firewalls, antivirus software, and encryption where necessary[2].

IT security is complex and ever-changing in response to threats. The best approach is normally to work with a trustworthy, highly-competent IT professional and give them the time and resources to implement the levels of security they feel appropriate.

iv. Access and permissions

Staff can pose a significant threat to information security either maliciously or accidentally. Restricting access to information is sensible and possible with most modern IT systems. You may need to restrict certain actions, for example, we usually encourage organisations to restrict the ability to bulk download data to a limited number of staff. It is also critical that a user's access to all IT systems can be instantly stopped, including access to systems hosted by third parties, either when the staff member poses a risk, or a security breach is threatened by the loss of a laptop or a password disclosed.

Again, the right balance needs to be struck between security and access when deciding user permissions. Although systems provide very fine-grained access permissions, we encourage clients to only restrict access to information where strictly necessary. We have found

https://doi.org/10.1017/S1472669610000125 Published online by Cambridge University Press

following a "need to know" policy frequently hinders legitimate access to information and affects business efficiency unnecessarily. In fact, national security departments in both the UK and US have changed in recent years from "need to know" policies to "need to share responsibly" recognising that failure to share information effectively can pose just as much of a threat to a country or organisation.

v. Transfer

Information can be at its most vulnerable whilst being transferred outside the organisation, as highlighted by some of the biggest government data losses[3]. Where it is necessary to transfer data, facilities and guidelines need to be provided to ensure it is transferred securely. Emailing, faxing, or downloading to USB memory sticks, CDs or laptops are all potentially high risk methods. Where it is unavoidable to store computer readable information on a mobile device, it should always be encrypted. Most importantly, the choice of method for transfer should be carefully considered and the most appropriate one chosen in each case.

Where regular transfer between two organisations or a dispersed team is required, using a secure, online system for storing and sharing documents can be one of the most secure, and easiest to use, solutions.

vi. Passwords and two-factor authentication

Even where information is encrypted, weak passwords are still a security flaw. A computer system can go some way to encouraging a secure password, for instance by insisting on a certain number of characters and including non-letter characters to stop dictionary words being used. However, without adequate staff training and staff choosing secure passwords[4], it is still a potential weakness.

To protect highly-sensitive information, for instance patient records, adding another access requirement, known as two-factor authentication, can help overcome the insecurity of passwords. For the private medical practice we introduced a token which is carried on a key-ring. When clicked it produces a one-time password required to access the system.

vii. Back-ups

Keeping information secure involves more than stopping unauthorised access, it requires information to be kept safe from accidental loss or destruction. Again, for smaller organisations, using a hosted solution means the service provider takes responsibility for backing-up your data. Anyone undertaking back-ups in-house needs to ensure that they are regularly taken (at least once a day), a back-up copy is stored at a separate location, and use of the backed-up data is tested (at least a few times a year.)

viii Disposal

Care should be taken when disposing of information or equipment used for processing information. IT equipment, particularly hard drives should be wiped and disposed of by specialists. Mobile phones and their SIM cards should be disposed of carefully not only because of the contact details on them but as they are frequently used to store passwords. Confidential, personal or sensitive information on paper should be shredded, disposed of in confidential waste bags and collected by specialist contractors.

ix Supply chain

Consider which other organisations have access to your information. For instance, cleaners in your office, IT companies who can access your system, document scanning bureaus, archive and storage companies, paper or hardware disposal companies. Ensure you have adequate contracts with them and they have similar measures to yours in place to ensure the security of your data[5].

When processing personal data, the data controller in your organisation remains responsible for all data processing even when done by third party contractors.

"Any enforcement or prosecution action for breaching the Data Protection Act will be against you as you are responsible for the processing of personal information by your outsourcer[6]."

x Physical space

Your physical working space also needs to be secure from deliberate or accidental data loss or theft. Practical measures include ensuring computer screens and passwords cannot be overlooked; fax machines, printers and photocopiers are in secure areas; telephone conversations cannot be overheard; and access to the building is secured.

4. Evaluation

The need to keep information secure and accessible and to get the right balance between the two, is an ongoing challenge that needs to be proactively managed. The person responsible for this in your organisation needs to keep up to date with changes in the law, with security threats, improving technology solutions, ensure new staff are trained, and check that all staff are following best practices. They need to ensure that everyone knows what to do in the event of a security breach and that there are adequate audit trails in IT systems and manual procedures so they can identify what went wrong, and if necessary, who was responsible.

Conclusion

Modern information technology offers great benefits to organisations, but this must be tempered with an understanding of the need for security. As more and more of an organisation's worth is bound up in electronic information and the ability to keep it secure, everyone has a responsibility to follow basic information security principles throughout their day-to-day work.

https://doi.org/10.1017/S1472669610000125 Published online by Cambridge University Press

References

[1]Norman, D.A. (2009) *When security gets in the way* [http://jnd.org/dn.mss/when_security_gets_in_the_way.html]
[2]For more on IT security see writings by Bruce Schneider http://www.schneier.com/
[3]Child benefit data was lost by HMRC, November 2007, when sent on CD to the National Audit Office. Home Office data about offenders was lost on an unencrypted memory stick, August 2008.
[4]For advice on choosing secure passwords see https://www.google.com/accounts/PasswordHelp
[5]For an illustration of data breaches in a supply chain see ITV's Tonight Programme report, Health Records For Sale, broadcast on 19 October 2009.
[6]McKilligan, NFJ and NHE Powell. (2009) *Data protection pocket guide: essential facts at your fingertips*. 2nd ed. London, British Standards Institute, p. 100.

Biography

Jennifer Smith is a qualified, chartered librarian. She worked for several years in legal information, both in commercial law firms and in legal education. She co-founded OneIS to provide smaller organisations with the technology and expertise to improve information management.

Legal Information Management, 10 (2010), pp. 54–57

doi:10.1017/S1472669610000228

Proving You're Worth It: Managing an Information Department in Challenging Times

Abstract: This article results from the Pre-Conference Seminar presented at the BIALL Conference in June 2009 by Victoria Jannetta and Pamela Wolffsohn. Having both raised their Information Department's profiles in a better economic climate, they shared how they created opportunities to establish good positioning in their firms. They also addressed the challenges we now face in these frostier times. This was a workshop and was brought to life by spirited discussions, potential solutions and ideas on how to deal with problems faced by many of us – reduced resources and headcount.
Keywords: information management; management skills; law firm libraries

Introduction

Victoria and I joined our firms, FFW (Field Fisher Waterhouse) and Nabarro LLP in the latter part of 2006, as managers of our Information Departments. The firms have similarities, both being medium-sized with some shared practice areas, Real Estate, Corporate, IP and Technology. We took different routes to establish a real presence in our firms and shared our success stories