imprivata®

Six key steps to help address data security in the world of GDPR

Data security has been an issue of concern in the health sector for a number of years, particularly following several high-profile data breaches. The matter has gained further prominence as a result of the EU wide General Data Protection Regulation (GDPR) being introduced around data protection along with various national IT security requirements and legislation. These regulations matter and apply to your organisation if you are storing or processing data.

Within hospitals there is widespread commitment to keeping data secure, however, there are still many instances of sub-standard practices which, without effective action, leave healthcare organisations exposed to risks as well as potential breaches of GDPR.

The consequences of data breaches can be substantial, not only financially, but also in the loss of public trust. GDPR introduces much larger fines which, whilst generally reserved for only the most serious breaches, can be as large as €20M or 4% of annual turnover. While some institutions may set aside money to recover from data breaches, hospitals generally cover such incidents with funds intended for patient care and healthcare improvements.

Technology can play a major role in helping healthcare organisations comply with GDPR and any required security standards. Here are six steps to help healthcare organisations meet those data protection and security recommendations.

1. Ensure your organisation has clear ownership and responsibility for data security and your processes are tested and externally audited

Leadership need to be visible and active in demonstrating clear ownership and responsibility for data security, in fact with GDPR, data controllers and data processors must name individuals who carry responsibility for data protection. CIOs have done an admirable job at protecting the perimeter, by securing the end-point. However, what most organisations can fail to acknowledge is that often the weakest link in the security chain is people. Targeting staff with phishing attacks (or one of the variants, such as spear phishing or whale phishing), lost or stolen devices, shared or generic user accounts, or via insecure lists of passwords (sometimes a sticky note), is the easiest way into an organisation's sensitive data.

This key first step should also apply to technology suppliers that healthcare organisations are planning to work with. Can the supplier demonstrate its credentials in managing technical, clinical risk and quality leadership?

2. Understand your organisation's vulnerabilities, and create a corresponding strategy for data security, compliance, education, and training

Healthcare organisations need to understand their vulnerabilities and their root causes that could lead to data breaches. In healthcare, typically, staff have too many complicated passwords, which they have to keep inputting in order to access clinical applications and patient records. This added complexity in a high-stress environment can lead to password sharing, shared or generic user accounts and other sub-optimal workarounds. Processes should be reviewed at least annually to identify and improve those which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Vulnerabilities to hacking attempts are complex and numerous. Education of staff will not solve the problem on its own, therefore, a technology solution is the best way to avoid a security breach, combined with education. A well-designed training program should take into consideration the IT skills and knowledge of system users, the impact on system change in their role, and identify how to mitigate the concerns of staff. By doing this, suppliers can help healthcare organisations to develop a culture of learning from examining mistakes and improving processes.

Vulnerabilities to hacking attempts are complex and numerous. Education of staff will not solve the problem on its own.

3. Ensure IT systems and data security protocols are designed around the needs of patient care and frontline staff

It is increasingly more likely that staff will be required to access an escalating number of applications, as more technology is introduced into hospitals. Logging into multiple applications takes time and often users can forget the many passwords they have to remember, prompting some to write down the password for each application, or keep them in unencrypted documents, which increases the security risk of an unauthorised person gaining access to an application.

By enabling easy and secure access to essential systems, clinicians can be more proactive, effective, and efficient in accessing the information. This enables more informed diagnosis and therefore less risk. Also, whilst GDPR does not contain any specific requirements around particular security methods, making access to systems simple and secure reduces the likelihood that staff will develop workarounds that will introduce further risk into the process and could lead to data breaches.

For example, a single sign-on solution to applications eliminates the use of passwords and the requirement to keep signing in, saving clinicians much needed time. Authentication management allows staff to access computers and mobile devices with the tap of a smart card or the swipe of a finger. When combined, staff are able to sign in once to gain access to all of the applications and accounts, without ever having to remember a password.

New technology such as virtual desktop infrastructure (VDI) provides greater flexibility, efficiency, intelligence, automation, and security, as well as being more cost-effective.

4. Safeguard against security issues by replacing out-dated hardware and software systems

Maintaining legacy systems can be costly and can lead to many problems. Legacy systems are more likely to be susceptible to malware and may be running operating systems that are impossible to patch or for which no patches are available. Outdated terminals may also be slow and unyielding, causing inefficiency for users in accessing data and systems. In addition to the security issue, legacy systems are a hindrance to innovation. New technology such as Virtual Desktop Infrastructure (VDI) provides greater flexibility, efficiency, intelligence, automation and security, as well as being more cost effective.

5. Reduce the risks of information loss by internally auditing and externally validating your data security processes

Internal data security audits allow an organisation to juxtapose the real-world, day-to-day practices against its documented policies, objectives, and procedures as well as being a fundamental need to ensure GDPR compliance. As already mentioned, internal audits highlight potential problem areas, that can then be mitigated before they cause issues. By conducting regular internal data security audits, and also seeking independent external validation, organisations can ensure they are strengthening their processes to a level similar to those assuring financial integrity and accountability. Through working with a supplier that has a deep understanding of information governance and clinical processes, healthcare organisations can verify that as well as meeting the day to day requirements of clinicians and patients, systems developed meet important governance requirements and reduce the risks of information loss.

6. Leverage existing knowledge and expertise by working with a supplier that understands the regulation

Healthcare organisations often struggle with justifying essential funding in IT solutions. By understanding security vulnerabilities, and the underlying root causes of those vulnerabilities, organisations can be more confident of selecting a solution that will address causes, rather than simply treating the symptoms. By working with a supplier that understands the regulations, healthcare organisations can leverage the knowledge and expertise of a supplier with real world experience. Suppliers with a proven track record can provide evidence of benefits realisation from workflow enhancement and assist in writing business cases that address end user needs and deliver productivity benefits. Additionally, good suppliers should act as trusted advisors, assisting healthcare organisations with addressing their information governance and security challenges, helping them be compliant, and helping them to meet the new data security standards.

The way forward

Over the last decade, healthcare has transitioned from a work place that was predominantly paper-based to one that is becoming digital. This evolutionary shift has delivered many benefits for patients, but it has also highlighted the need to ensure electronic patient health records are kept secure at all times.

With GDPR and national IT security requirements, healthcare organisations must take steps to understand their individual exposure to risk and act to reduce it as a matter of urgency. By working with a technology supplier that understands the challenges, healthcare organisations can ease the process towards digital transformation.

With GDPR, healthcare organisations must take steps to understand their individual exposure to risk and act to reduce it as a matter of urgency.

imprivata®

About Imprivata

Imprivata, the healthcare IT security company, enables healthcare securely by establishing trust between people, technology, and information to address critical compliance and security challenges while improving productivity and the patient experience.

For further information please contact us at

1 781 674 2700
or visit us online at
www.imprivata.com/intl

Offices in

Lexington, MA USA
Uxbridge, UK
Melbourne, Australia
Nuremberg, Germany
The Hague, Netherlands

OS-WP-SixStepsGDPR-0618-intl