Business efficient security for health
Enabling the delivery of care and treatment whilst protecting patient data
Executive summary

Healthcare technologies must protect patient data, as well as support care and treatment.

Privacy, security and confidentiality are red hot topics in the healthcare sector. Sensitive personal data has to be kept safe from unauthorised access, misuse, corruption and loss. The law demands this and patients expect this.

Yet, at the same time, the healthcare sector needs to be efficient and productive. Security cannot become a barrier to the delivery of patient care. In life and death situations and cases of urgency doctors, nurses and paramedics should not be impeded by archaic technological processes, or unnecessary worry about compliance with confidentiality, privacy and security law.

In this paper we identify and discuss the core legal framework for confidentiality, privacy and security in the UK and Europe, looking at how these topics are regulated and how the law treats failure. Our core proposition is that the law requires the healthcare sector to adopt ‘Privacy and Security Enhancing Technologies’ (‘PETs’ and ‘SETs’), but in order to satisfy the primary duty of care owed to patients, which is to afford them speedy and appropriate treatment, these technologies must be ones that are ‘business enabling’. Both issues must be addressed in the procurement process and during the design of technology architectures. Focussing simply on the privacy and security considerations at the expense of efficient delivery of healthcare is legally unsustainable. PETs and SETs must also help to lower the barriers to patient care and treatment.

In this paper we will also outline what organisations are required to do in practice to protect patient data (based on UK and European enforcement action and guidance) and identify core functionality that can help organisations meet those requirements in a business efficient way.

Imprivata

This white paper has been commissioned by Imprivata, the market leader in secure access and collaboration technologies for healthcare. Visit http://www.imprivata.com/ for more information.

EU privacy law is changing. If you fail to keep patient data private, secure and confidential, you could be fined up to 5% of worldwide annual turnover, which will cause significant brand/reputational damage and will result in financial pain.
**Our core proposition**

Healthcare providers should adopt Privacy and Security Enhancing Technologies (‘PETs’ and ‘SETs’) that enable healthcare, rather than placing unnecessary barriers to care and treatment in the way of doctors, nurses and paramedics.

Healthcare providers are totally reliant on electronic systems for the processing of patient data. Patient records contain some of the most sensitive and private information about individuals that is imaginable. Without appropriate PETs and SETs in place, there is an obvious risk that patient data will be accessed and used unlawfully.

The privacy and security of patient data is now subject to heightened public interest and regulatory attention, following many high profile cases of privacy and security breaches.

The law now has a very low tolerance for lapses of privacy and security in the healthcare sector.

This is evidenced in the enforcement action taken by regulators and in court judgements across Europe. Failure to comply with the law can lead to very serious legal consequences, including criminal prosecutions, penalties and sanctions, and significant operational challenges, such as business disruption, financial loss and damage to brand and reputation. In the last 3 years, the Spanish data protection authority has issued fines of over €40 million and the UK data protection regulator has issued fines of over £5 million for breaches of data protection law. These figures will be significantly higher when the proposed mega fines in the draft EU Data Protection Regulation are approved.

As healthcare organisations adopt new technologies and introduce more applications, each with their own privacy and security features and requirements, patient care and treatment may be impeded by doctors and nurses being subject to multiple login and authentication requirements resulting in more time being spent logging into systems and less time caring for patients. Each new layer of login and authentication introduces another new barrier to productivity and efficiency. In healthcare, particularly in emergency situations, productivity and efficiency is a vital consideration and very often a life and death matter. What healthcare organisations need is business-enabling privacy and security technologies. Technologies should protect the privacy and security of patient data in ways that are practical to use and which facilitate rather than inhibit productivity and workflow.

Compulsory privacy and security audits of the NHS

In February 2015 the UK government amended the Data Protection Act, to give the Information Commissioner the power to perform compulsory privacy and security audits of the NHS. This power reflects the priority that the law affords to the maintenance of the privacy and security of patient data. NHS bodies will need to be able to demonstrate to the Commissioner’s auditors that they have adopted appropriate Privacy and Security Enhancing Technologies (PETs and SETs).
Patient confidentiality and trust, at the heart of all patient-doctor relationships

The patient-doctor relationship is based on trust. Patients need to trust that anything said to the doctor remains private and confidential. If this trust did not exist, the patient may not be willing to seek medical help and may not feel able to speak openly. This trust comes from the doctor’s duty of confidentiality to the patient. Indeed, the patient-doctor relationship is the archetypal relationship to which confidence attaches. This duty of confidentiality can be traced back over 2,500 years to the Hippocratic Oath, which established confidentiality as an essential element of the moral code of conduct for doctors. It requires doctors to hold whatever they “may see or hear in treatment, or even without treatment… to be unutterable”. In 1948, the General Assembly of the World Medical Association adopted the Declaration of Geneva as a revision to the Hippocratic Oath to be understood and recognised in a modern way. Part of the declaration includes a requirement for doctors to “... respect the secrets that are confided [in them] even after the patient has died.” Organisations responsible for supervising doctors reinforce this in their standards and ethics guides. Professional standards followed by healthcare professionals all over the world contain similar requirements to keep patient information confidential. The duty of confidentiality imposed on healthcare professionals applies both to information obtained directly from patients and from other sources, for example, other medical staff and information imparted in the treatment of patients and their medical records. Any breach of this duty of confidentiality would unquestionably cause substantial distress for the patients affected by the breach.

Confidentiality is vital to secure public as well as private health
In the case of X v Y & Others [1988] it was observed that “The public in general and patients in particular were entitled to expect hospital records to be confidential and it was not for any individual to take it upon himself or herself to breach that confidence...”

World Medical Association International Code of Medical Ethics (The Declaration of Geneva)
At the time of being admitted as a member of the medical profession, physicians promise that: “the health of my patient will be my first consideration; and I will respect the secrets that are confided in me, even after the patient has died.”
Confidentiality as a matter of law

Duty of confidence

It is well-established that confidential information is protected by the doctrine of confidentiality. The general principle is that anyone receiving information in confidence should not be able to take unfair advantage of it. The following elements are required to establish a breach of a duty of confidence as set out in the case of Coco v Clark: (i) the information must have a necessary quality of confidence (i.e. not be trivial or public); (ii) the information must be imparted in circumstances importing an obligation of confidence (for example, where there is a confidential relationship such as a patient-doctor relationship); and (iii) there must be a breach of that confidence by the person receiving the information which causes a detriment to the person imparting it. It is recognised that the doctrine of confidentiality applies to medical information (X v Y & Others) [1988].

Human rights

Privacy is a fundamental human right recognised by international law. The European Convention on Human Rights is an international treaty signed and ratified by the members of the Council of Europe. It aims to protect basic human rights and fundamental freedoms. Article 8 of the European Convention on Human Rights sets out the right to respect a person’s private and family life, home and correspondence (an express right to privacy). Under the European Convention on Human Rights, it is unlawful for public bodies, and those performing functions of a public nature, to act in a way that...
is incompatible with the European Convention on Human Rights. This means that health organisations (who are likely to be public bodies or performing functions of a public nature) must act in a way that is compatible with the right to privacy. European Court of Human Rights cases have established that the right to privacy protects health data.

In the UK, The Human Rights Act 1998 gives effect to the European Convention on Human Rights. The Human Rights Act 1998 requires the courts to act in a way that is compatible with the European Convention on Human Rights and take account of European Court of Human Rights case law. In the case of Campbell v Mirror Group, the House of Lords used article 8 of the European Convention on Human Rights to extend the law of confidence to cover the wrongful disclosure of private information. Lord Nicholls stated that “the values enshrined in articles 8 and 10 [of the Human Rights Act 1998] are now part of the cause of action in breach of confidence.” Another notable principle that was established in the case is that the Human Rights Act 1998, including the right to privacy, is as applicable between individuals and organisations as it is between individuals and public bodies. In a case for misuse of private information, the question a court will ask is whether there is a reasonable expectation of privacy. If there is, it is a breach of confidence not to respect that right of privacy. Unlike an action for breach of the duty of confidence, there is no need for the existence of a confidential relationship to bring an action for wrongful disclosure of private information and importantly the focus of the action is not on the confidentiality of the information, but on intrusion. This means that personal information can still be afforded protection after it has been disclosed and is no longer secret.

Failure to comply with the law can lead to very serious legal consequences, including criminal prosecutions, penalties and sanctions, and significant operational challenges, such as business disruption, financial loss and damage to brand and reputation.

**Data protection**

Data protection laws have extended the statutory protection of privacy in relation to personal data. Personal data is now subject to an extensive statutory and regulatory regime. The Council of Europe Convention 108 which came into force in 1981 was the first international legally binding instrument dealing explicitly with data protection. It sets out a core set of principles that organisations must follow. Personal data must be: (i) obtained and processed fairly and lawfully; (ii) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (iii) adequate, relevant and not excessive in relation to the purposes for which they are stored; (iv) accurate and, where necessary, kept up to date; (v) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. Personal data concerning health is afforded special protection. Council of Europe Convention also highlights data security as a key area of focus when handling personal data. Appropriate security measures must be taken for the protection of personal data against accidental or unauthorised destruction or accidental loss as well as...
against unauthorised access, alteration or dissemination.

Under EU law, data protection was regulated for the first time by the Data Protection Directive. The aim of the Directive is to provide a consistent approach to protect the privacy of personal data held in computerised and manual files. It outlines a standard that data controllers (those that decide the manner and purpose of which data processed) have to adhere to when they process personal data in the form of a set of principles. These principles are based on the principles set out in the Council of Europe Convention. Sensitive personal data is subject to stronger protection under the Directive. The Article 29 Working Party, an independent European advisory body on data protection and privacy, is of the opinion that all data contained in medical documentation, in electronic health records and systems should be considered to be “sensitive personal data”. Each country in Europe has its own legislation implementing the Data Protection Directive. For example, in Germany, the Federal Data Protection Act (Bundesdatenschutzgesetz) implements the EU Data Protection Directive and, in the France, the Data Process Act implements the EU Data Protection Directive.

A further layer of protection for privacy and personal data is included in the EU Charter of Fundamental Rights (EU Charter), which assembles the fundamental rights protected in the EU within one document. The EU Charter became legally binding on all EU member states in December 2009 with the entry into force of the Treaty of Lisbon. It recognises privacy and data protection as fundamental rights. Under the EU Charter, everyone has the right to respect for his or her private and family life, home and communications and everyone has the right to the protection of personal data concerning him or her, which must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone also has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

**Interim conclusion – there is a clear legal duty to protect health data**

This analysis of the legal landscape clearly shows that there is strong legal protection for confidential information, personal information and personal data in Europe. The law of confidence, the human rights regime, particularly the right of privacy and the Data Protection Directive (implemented in national legislation across Europe) all establish legal mechanisms for the protection of health data. The result is that organisations handling health data have a clear legal duty to protect that data.

**European law: Hospital failure to control access to health records is a violation of European Convention on Human Rights**

In the case of I v Finland, the European Court of Human rights awarded damages and costs of over €30,000 to a patient for violation of the Article 8 right to privacy in the European Convention on Human Rights because the hospital failed to restrict access to electronic health records to those health professionals directly involved in treatment, and failed to maintain a log of all persons who had accessed medical files.
So what does the duty to protect health data look like? A number of high profile data security breaches over the last few years have put data security at the forefront of regulatory action in relation to data protection (see the table of Information Commissioner’s Office health enforcement actions). By analysing the case law, regulatory action and guidance, it is clear that there is a set of core duties for organisations and requirements that must be implemented to comply with those duties. The law demands that personal data, and in particular, health data must be kept safe from unauthorised access, misuse, corruption and loss and the following paragraphs set out what this means in practice.

In Spain, there is specific legislation in relation to security of and access to medical records, which states that access to patients’ medical records should be limited to healthcare professionals obliged to maintain professional secrecy, as well as employees that need access in order to exercise their functions. The Italian Data Protection Authority sets out technical arrangements that organisations must have in place to ensure the security of electronic health records in its Guidelines on the Electronic Health Record and the Health File. These include, applying suitable authentication and authorisation systems, putting in place procedures to regularly check quality and consistency of authentication credentials and authorisation profiles, implementing criteria to encrypt and/or keep separate the data disclosing health and sex life from other personal data, logging access and operations and putting in place audit logging to control database access and detect abnormalities. Under the Data Protection Directive, European organisations are also obliged to have “regard to the state of technological development” and review the measures they have in place periodically to keep abreast of technological developments. This means that healthcare providers must consider the technologies that are on the market or they risk regulatory or citizen action for breach of their duty.

One of the main reasons for regulatory action across Europe is breach of the requirement to take appropriate technical

### Table of Information Commissioner’s Office health enforcement actions

<table>
<thead>
<tr>
<th>Healthcare cases</th>
<th>Monetary Penalty Notices (Fines)</th>
<th>Prosecutions</th>
<th>Enforcement Notices</th>
<th>Undertakings</th>
<th>Total number of actions</th>
<th>Total actions as a% of all enforcement actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. % of total</td>
<td>No. % of total</td>
<td>No. % of total</td>
<td>No. % of total</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>7 28%</td>
<td>1 17%</td>
<td>0 -</td>
<td>5 16%</td>
<td>10</td>
<td>20%</td>
</tr>
<tr>
<td>2013</td>
<td>4 22%</td>
<td>1 14%</td>
<td>0 -</td>
<td>5 22%</td>
<td>10</td>
<td>19%</td>
</tr>
<tr>
<td>2014</td>
<td>1 9%</td>
<td>1 6%</td>
<td>2 18%</td>
<td>12 41%</td>
<td>16</td>
<td>19%</td>
</tr>
</tbody>
</table>
and organisational measures. Over the last few years fines for breaches of the security principal have been the highest fines issued by the Information Commissioner’s Office (£325,000 in 2012, £250,000 in 2013 and £200,000 in 2014). Organisations taking a risk-based approach to privacy and security must prioritise security over everything else if they want to minimise the risk of action by regulators and citizens.

The Caldicott Report, which was commissioned by the Chief Medical Officer of England due to concerns about the ways patient information is used in the National Health Service, recommended a set of key principles to be followed by organisations with access to patient information to provide a framework of good practice. One of the principles is that access to patient-identifiable information should be on a strict need-to-know basis. It is, therefore, essential that systems have a mechanism for ensuring that only appropriate health professionals gain access to patient information for legitimate purposes related to the care of the patient. The European Court of Human Rights case of I v Finland found that it was a breach of the article 8 right to privacy for a public hospital to fail to have access controls in place. The obligation to have access controls in place includes protecting patient data after it has been accessed. In a healthcare context, this must include a mechanism to restrict access to patient data if a healthcare professional leaves their workstation (for example, in an emergency). Security and privacy of patient data must not be denied in emergency situations when there is technology that exists to eliminate the risk (for example, technology that automatically secures the workstation when the user walks away).

In practice, this can be achieved by having appropriate authentication, authorisation and audit mechanisms in place to control access to electronic patient data. The Article 29 Working Party has published a Working Document on the processing of personal data relating to health in electronic health records, which recommends implementing “a reliable and effective system of electronic identification and authentication as well as constantly up-dated registers for checking on the accurate authorisation of persons with access” to patient records. Strong authentication using electronic signatures together with official identification (e.g. smart cards) is envisaged by the Article 29 Working Party to “avoid the known risks of password authentication”. To provide effective security, the authentication method must prove both the identity of the user and their role (e.g. surgeon, nurse, receptionist) to be able to apply appropriate rights of access to patient data on a need to know basis. Regulatory guidance and actions have established encryption as an essential technical security measure to protect personal data. The Information Commissioner’s Office identifies encryption as a “means of ensuring that data can only be accessed by authorised users” in its Practical Guide to IT Security and the Article 29 Working Party has mandated that for health data “encryption should not only be used for transfer but also for storage of data in systems”.

Monitoring and reporting of user actions has been mandated in the decision of I v Finland, in which it was held that it was a breach of the article 8 right to privacy for a public hospital to fail to have a system in place to log information on the staff members who had accessed patient records. So it is clear that health organisations must keep an audit trail of those who have access to patient records or they risk regulatory or legal action. The Article 29 Working Party further recommends “comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorisation.”

Human error is one the greatest vulnerabilities within an organisation when it comes to security. Having user-friendly systems, training staff and implementing policies around data protection, privacy and cyber security is a way of minimising the risk of human error (although it will never be eliminated). In relation to electronic health systems, the Article 29 Working Party recommends issuing “clear and documented instructions to all authorised personnel on how to properly use systems and how to avoid security risks and breaches.”

One of the biggest weaknesses of existing security systems in healthcare is that they are often not easy to use. If security is a barrier, staff will find a way to work around it. Multiple and complex passwords mean that staff write them down in order to remember them (increasing the risk of unauthorised access to patient data). Lengthy login procedures mean that users share sessions instead of logging in and out of workstations using their own unique credentials, which breaches the requirement that access to patient data is on a strict need to know basis and to have a log of who has accessed data. Healthcare organisations have a clear duty to ensure that staff work in a way that complies with the law. We believe that this duty means

---

**Global enforcement: Regulators are becoming more sophisticated and citizens are becoming more savvy**

Privacy and security regulators are cooperating on a monumental scale to protect privacy across borders. In 2014, the Global Privacy Enforcement Network (created to strengthen personal privacy protections in a global context ) continued to sign-up new national regulators, like the US Federal Communications Commission and created an official contractual framework for its combined efforts. It is clear that the Information Commissioner’s Office is taking a more rounded view to the use of its enforcement powers. There has been a marked shift away from attention-grabbing financial penalties, to more subtle – and some might say more effective – enforcement tools, namely Enforcement Notices and Undertakings. However, the number of enforcement cases has remained fairly constant over the past three years in terms of the volume of concluded cases. Some of the biggest cases in Europe in 2014 involve citizen activists pushing their cases to the court of justice of the European Union. With the new Data Protection Regulation on its way, organisations need to prepare for even further scrutiny from regulators and citizens (as their powers are strengthened) and for bigger fines of they get it wrong.
providing efficient, easy to use security in order to minimise the risk of staff working around the measures in place (and controls to monitor if they do), which in turn will reduce the likelihood of breaches resulting from human error. Training staff and making it easier for them to act in the correct way by implementing security measures that facilitate workflow is the best solution to the problem of human error and the weaknesses in many existing systems.

**Recent enforcement action in health**

Each country in Europe has a data protection authority charged with regulating and enforcing data protection. These national regulators have a toolbox of enforcement powers at their disposal. These include the ability to issue fines for breaches of the law (for example, the data protection authorities in Spain, France and Slovenia can issue fines of up to €600,000, €1,500,000 and €1,000,000 respectively), enter premises and inspect documents, demand documentation and information (for example, the French data protection authority has the power to request copies of all documents it deems useful to its investigation), stop organisations from processing personal data and order organisations to make changes (for example, implement staff training and security measures). In many countries, there is criminal liability for failure to comply with the law which can result in imprisonment (for example, in Italy failure to provide minimum security measures can result in imprisonment of up to two years or a fine of up to €120,000). On top of this national courts and European courts can hear claims for breaches of privacy and confidentiality which are increasingly instigated by individuals enforcing their rights. Some examples of recent enforcement actions in health are outlined below.

The Information Commissioner’s Office has taken regular enforcement action and issued a number of monetary penalty notices (fines) to health organisations since 2012 for not keeping health data secure. In 2012, the Information Commissioner’s Office issued a record fine of £325,000 to Brighton and Sussex NHS Trust after an investigation found that hard drives previously owned by the Brighton and Sussex NHS Trust containing sensitive personal information were made available for sale without having been properly erased. More recently, NHS Surrey was fined £200,000 for not taking appropriate steps to safeguard sensitive personal information.

In 2014, the Italian Data Protection Authority ordered a public hospital to implement systems to restrict access to patient data only to those professionals/departments who provide care to the patient and, in Germany, the data protection authority publicised that a health insurer was fined €1,300,000 (and ordered to make a further donation of €600,000 towards research on improving data protection) for using personal data unlawfully.

**Collaborative working in health – one of the main reasons for privacy and security fines**

The provision of patient care and treatment rests on collaborative working, between different physicians, treating organisations, related service providers and across national boundaries. In life and death situations and other urgent situations, the efficiency of collaboration can make all the difference.

Unfortunately, many of the high profile data protection cases in the UK in recent years have concerned bad working practices for collaborative working in the healthcare sector, which have resulted in sensitive personal data being improperly disclosed to third parties, or being delayed in their transmission to the intended recipients. Typical problems have concerned data mishandling cases involving the use of fax machines, photocopiers and email.

Healthcare providers need to ensure that they adopt robust systems that support the privacy and security of patient data throughout all collaborative working practices. Collaboration is vital to the discharge of the legal duties for proper care and treatment, but it should comply with the Data Protection Act too.

The Dutch Data Protection Authority recently expressed concern over inadequate security measures in the health sector after it carried out a major investigation and found that medical records were accessible by people with whom patients had no treatment relationship due to inadequate security measures.

Recent health enforcement actions in Spain include penalty proceedings and the declaration of infringement proceedings by the Spanish Data Protection Authority. The Spanish Data Protection Authority started penalty proceedings against a health care centre, after several plastic bags were found in the street containing files with personal data from the centre’s patients, including sensitive information in relation to the patients’ health, which resulted in a fine. Declaration of infringement proceedings were initiated by data subject’s claim against a public hospital (government body). It was proven that documentation containing personal data of the complainant was lost, which resulted in the Spanish Data Protection Authority declaring a serious infringement of data protection law by the public hospital. It is important to highlight, that in accordance to the Spanish Data Protection legislation, public administrations are not fined, for that reason the declaration of infringement was made and corrective measures had to be implemented by the offender.

In 2014, the Italian Data Protection Authority ordered a public hospital to implement systems to restrict access to patient data only to those professionals/departments who provide care to the patient.
The implementation of appropriate technical security measures (as outlined above) is necessary to ensure compatibility of systems with fundamental rights.

The costs involved should be seen by organisations as an essential investment to extend the relationship of trust between patients and healthcare professionals into the electronic/automated world.

The Article 29 Working Party acknowledges that electronic health record systems “have the potential to achieve greater quality and security in medical information than the traditional forms of medical documentation”. In the healthcare sector, unauthorised access to systems must be practically impossible in order to satisfy legal privacy, security and confidentiality obligations but practically unrestricted in cases of emergency where there is a genuine need to access the patient information. In our opinion the right technology can satisfy the legal obligations faced by health organisations and meet the competing requirements of restricted/unlimited access whilst improving productivity and efficiency.

The case law and regulatory guidance across the EU make it clear that organisations need technology solutions with the following functionality:

- strong authentication and access controls appropriate to the organisation’s security requirements (such as biometrics, proximity cards, smart cards and one-time password tokens); and
- the ability to monitor and report on user actions.

Productivity and efficiency can be improved by selecting technology solutions that support workflow and are simple and easy to use. This has the effect of improving productivity and efficiency of staff as well as reducing the risk that staff will look for ways to work-around the security measures in place.

Healthcare organisations need technology solutions that support their staff’s workflow which involves workstation sharing, the need to rapidly access information, simple authentication and a mechanism for safeguarding unattended workstations. There is functionality available on the market that optimises workflow efficiency and the delivery of care to patients while providing the technical security measures demanded by the law (user secure access on a need to know basis, strong authentication, post event monitoring and audit). Some examples of functionality that will enable health organisations to meet legal obligations and provide efficient patient care.

Single sign-on functionality that manages application credentials provides secure access controls while eliminating the time and effort for users to enter multiple usernames and passwords each time they need to access an application. Single sign-on facilitates workstation sharing and rapid access to information, which are key to the efficient provision of healthcare. This functionality also provides secure access controls and is easy for staff to use so minimises the risk that staff will write down their passwords or share logon sessions which would breach the healthcare organisation’s legal obligations.

Strong means of authentication using a combination of authentication factors such as facial recognition, fingerprints, smart cards, proximity cards and a password or pin are available to grant users fast access to applications. This results in increased efficiency in the delivery of patient care while protecting patient data.

Functionality that automatically secures workstations when users walk away and automatically re-authenicates users when they return using facial recognition and detection technologies. This means that patient data is secured if a doctor needs to leave a workstation in an emergency but it is quick for the doctor to access the workstation again when they return, resulting in increased efficiency. The variety of authentication management solutions available means that there is likely to be a solution available to fit each organisation.

EU privacy law requires you to implement robust technologies for maintaining security, limiting access, keeping records of access and auditing. Strong authentication and access control technologies in the healthcare sector are compulsory functionalities as a matter of law.
**Conclusion**

The law demands that health data is protected and case law, regulatory action and guidelines in relation to the health sector set out a clear set of measures that organisations must take to comply with their duties. Security is a key focus for the protection of health data but to operate effectively, healthcare organisations need business-enabling security. There are a number of technology solutions available to healthcare organisations to help them to comply with their duties without disrupting the business.

---

*European law: Processing of personal data relating to health in electronic health records*

The Article 29 Working Party outlines the following safeguards as a necessity in relation data security of electronic health records (EHR):

- “the development of a reliable and effective system of electronic identification and authentication as well as constantly up-dated registers for checking on the accurate authorisation of persons having or requesting access to the EHR system;

- comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorisation;

- effective back up and recovery mechanisms in order to secure the content of the system;

- preventing unauthorised access to or alteration of EHR data at the time of transfer or of back up storage, e.g. by using cryptographic algorithms;

- clear and documented instructions to all authorised personnel on how to properly use EHR systems and how to avoid security risks and breaches;

- a clear distinction of functions and competences concerning the categories of persons in charge of the system or at least involved in the system with a view to liability for shortcomings;

- regular internal and external data protection auditing.”

PwC Legal - Who we are

PwC Legal provides business-critical support on data protection, privacy, confidentiality and security matters to businesses, governments and public authorities all over the world. Working closely with audit, consulting, risk management and forensics experts in all parts of the PwC global network, we provide an end-to-end, seamless service that is unrivalled in the market. We support clients with: the development of their strategies for data handling and use; the development and management of national and international compliance projects; Data Protection Officer services, outsourcing and cosourcing; regulatory liaison and clearance; incident response and breach disclosure; regulatory investigations and enforcement actions; civil and criminal litigation; and crisis management.

About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata’s Single Sign-On and Authentication Management enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care.

Over 2 million care providers in more than 1,000 healthcare organisations worldwide rely on Imprivata solutions.

Business case development

We highlight the following points to help healthcare organisations with the development of their business cases for the procurement of new technologies:

- Competing legal duties: Technologies must support the delivery of care and treatment, not create barriers or obstacles for doctors, nurses and paramedics. Technologies must also help to protect the privacy and security of patient data. Therefore, these duties must be considered together, whenever procurement options are being weighed-up.

- Data protection law is actively enforced against healthcare providers. The Information Commissioner regularly takes enforcement action against healthcare providers for failing to adequately protect the privacy and security of patient data. Financial penalties are regularly imposed in serious cases.

- Data protection law is undergoing a process of amendment in the EU, with a particular focus on the security of patient data. The EU is currently amending the Data Protection Directive, to introduce new security requirements, including obligations for mandatory reporting of serious privacy and security breaches to regulators and people affected.

- The functionality of technologies required for compliance with data protection law is already clear. As well as encryption of sensitive data, the law requires access controls, user authentication and the keeping of logs of systems use, for audit purposes.
### Security breach transparency in Europe

EU data protection law requires controllers of medical information to report security and privacy breaches to data protection authorities and people affected. For example:

<table>
<thead>
<tr>
<th>Country</th>
<th>Regulation/Applicable Law</th>
<th>Summary of impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Federal Act concerning the Protection of Personal Data (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000))</td>
<td>If a data controller becomes aware of a serious data breach which may result in damage to data subjects, the data controller must notify the data subjects in an appropriate manner. This is subject to a proportionality principle.</td>
</tr>
<tr>
<td>Belgium</td>
<td>Good practice to notify the Belgian Data Protection Authority (BDPA) (based on the data protection authority’s interpretation of the EU Data Protection Directive)</td>
<td>Best practice is to notify the BDPA who may then chose to notify the data subjects.</td>
</tr>
<tr>
<td>Denmark</td>
<td>Data protection authority’s interpretation of the EU Data Protection Directive</td>
<td>Good practice to notify data subjects upon ‘unintended publication’ of personal data.</td>
</tr>
<tr>
<td>France</td>
<td>Proposed amendment to article L. 111-8-2 of the French Public Health code</td>
<td>If the proposed amendment is enacted, it would lead to a new obligation for health entities to report any serious health data breach to the French Health Regional Authorities</td>
</tr>
<tr>
<td>Germany</td>
<td>Section 42, Federal Data Protection Act (Bundesdatenschutzgesetz)</td>
<td>The relevant authority and individual data subjects must be notified in the event of particularly sensitive data breaches where there is a serious threat of interference with the interests of the relevant data subjects.</td>
</tr>
<tr>
<td>Greece</td>
<td>Greek Data Protection Authority (GPDA) guidance and directions</td>
<td>The GDPA encourages the voluntary reporting of breaches, which may help data controllers avoid further action or imposition of fines upon GDPA review.</td>
</tr>
<tr>
<td>Ireland</td>
<td>Personal Data Security Breach Code of Practice (2010) published by the Data Protection Commissioner (DPC) under s.19(2) (b) of the Data Protection Acts 1998 &amp; 2003</td>
<td>Data controllers must contact the DPC upon discovery of a breach. In addition, data controllers must consider whether to inform data subjects depending on the nature and circumstances of the breach.</td>
</tr>
<tr>
<td>Netherlands</td>
<td>A draft bill has been approved by the Dutch Second Chamber implementing mandatory breach disclosure to the data protection authority and data subjects in the event of severe negative effects</td>
<td>If the bill becomes law, the data protection authority and data subjects must be notified in the event of data breaches resulting in severe negative effects.</td>
</tr>
<tr>
<td>Sweden</td>
<td>S.38 Swedish Personal Data Act (Sw. Personuppgiftslagen (1998:204))</td>
<td>General obligation of the data controller’s Data Protection Officer to inform the Swedish Data Protection Authority of any suspected breaches of the Swedish Personal Data Act.</td>
</tr>
<tr>
<td>UK</td>
<td>Health and Social Care Information Centre (&quot;HSCIC&quot;) Checklist Guidance for Reporting, Managing and Investigating Information Governance (&quot;IG&quot;) and Cyber Security Serious Incidents Requiring Investigation (&quot;SIRI&quot;) (version 5.0 published on 27 February 2015)</td>
<td>Applicable to all organisations processing Health, Public Health and Adult Social Care Personal Data. All health service organisations in England must use the IG Toolkit Incident Reporting Tool and report IG SIRIs to the HSCIC, Department of Health, UK data protection authority and other regulators.</td>
</tr>
</tbody>
</table>
### Requirement to control access to personal data and systems in Europe

Data protection law requires controllers of personal data to control access to personal data and systems. For example:

<table>
<thead>
<tr>
<th>Country</th>
<th>National legislation reference</th>
<th>Requirements to control access to personal data and systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000) Section 14, paragraph 2(4), (5) and (7)</td>
<td>Access to and use of (1) the premises of the data controller or processor; (2) the data; and (3) programs relating to the same (by authorised persons) must be restricted. Logs must be kept to ensure that the permissibility of the data processing steps that were performed can be traced.</td>
</tr>
<tr>
<td>Belgium</td>
<td>Belgian Law of 8 December 1992 on Privacy in relation to the Processing of Personal Data as modified by the law of 11 December 1998 implementing Directive 95/46/EC and the law of 26 February 2003 Article 16, para 2(2)</td>
<td>Access to personal data processed by people acting under the data controller’s authority must be limited to what is necessary for the fulfilment of their duties or for the requirements of the service.</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Personal Data Protection Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts Article 13(4)(a)-(d)</td>
<td>Ensure that systems used for automatic processing of personal data are used only by authorised persons. Authorised persons may only have access to the personal data corresponding to their authorisation on the basis of specific user authorisations established exclusively for these persons. Electronic records should be able to identify and verify when, by whom and for what reason the personal data were recorded or otherwise processed and prevent any unauthorised access to data carriers.</td>
</tr>
<tr>
<td>Estonia</td>
<td>Personal Data Protection Act (12 February 2003) Section 19, subsection 2 and 3</td>
<td>Access to equipment used for processing personal data by unauthorised persons must be prevented. Ensure that it is possible to determine when, by whom and which personal data were recorded, altered or erased. Ensure that every user of a data processing system has access only to personal data to which the user is permitted to process.</td>
</tr>
<tr>
<td>Germany</td>
<td>Federal Data Protection Act (15 November 2006) Annex 9(1),(2),(3) and (5)</td>
<td>Required to (1) prevent unauthorised persons from gaining access to data processing systems with which personal data are processed; and (2) prevent these systems from being used without authorisation. Ensure that persons entitled to use personal data processing systems have access only to the data to which they have a right to access. Ensure that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage. Ensure that it is possible to check and establish whether and by whom personal data have been inputted into data processing systems, modified or removed.</td>
</tr>
</tbody>
</table>
### Italy

**Personal Data Protection Code**  
Legislative Decree no.196 of 30 June 2003  
Section 34(a)-(3)  
Section 35(c)  
Annex B

Annex B includes detailed and prescriptive requirements regarding security measures to be implemented, including access control measures.

For example, persons are allowed to process personal data by electronic means (and therefore have access to such data) only if they are provided with authentication credentials. This would consist of an ID code for the person in charge of the processing and a “secret” password eight characters long only to be known by that person. These authentication credentials must be de-activated if the said person is disqualified from accessing personal data.

### Luxembourg

**Data Protection Act (2 August 2002 as amended)**  
Article 23

Required to (1) prevent any unauthorised person from accessing the facilities used for data processing; (2) prevent data media from being read, copied, amended or moved by any authorised persons; and (3) prevent unauthorised introduction of any data into the information system, as well as any unauthorised knowledge, amendment or deletion of the recorded data.

Ensure that the identity of persons having had access to the information system and the data introduced into the system can be checked and recorded at any time and by any person.

Ensure that authorised persons may only access data that are within their competence.

### Portugal

**Data Protection Act (26 October 1998 no.67)**  
Article 15

Required to (1) prevent unauthorised persons from entering the premises used for processing personal data; (2) prevent data media from being read, copied, altered or removed by unauthorised persons; and (3) prevent unauthorised input and unauthorised obtaining of knowledge, alteration or elimination of personal data.

Ensure that authorised persons may only access data covered by the authorisation and that it is possible to check which personal data were inputted, when and by whom.

### Spain

**Personal Data Protection Act 2004**  
Article 91 and 93

In Spain, there are three levels of security measures: basic, medium and high. Basic level security measures must be adopted as a minimum. Depending on the nature of personal data processed and by whom, medium and high security measures must also be considered and implemented – this is the case for personal data relating to health as it is classified as “sensitive” personal data.

Examples of requirements in relation to access controls are as follows:

- users must only have access to those resources required for the performance of their functions;
- the data controller must ensure there is an updated list of users and user profiles and the authorised accesses for each one;
- the data controller shall establish mechanisms to avoid a user being able to access resources with rights other than those authorised;
- only staff members authorised in the security document shall grant, alter, or annul the access authorised to resources, pursuant to the criteria established by the data controller;
- should personnel not pertaining to the data controller have access to the resources, they must be subject to the same security conditions and obligations as the internal personnel; and
- the data controller must establish a mechanism that permits the unequivocal and personalised identification of any user who tries to access the information system and the verification of his authorisation.