Patient privacy across the European Union

Ed Percy, with help from Michel Boivin and Ross Cardew

2014 Conference of the MUHC-ISAI: Patient Engagement: What is it?
Why does it matter? How is it done? October 3, 2014

CGI

Experience the commitment®

Objectives of the presentation

Through sharing best practices and global experiences, the audience will gain an understanding of how European patient privacy legislation has evolved, and an idea of the challenges posed by ‘services at a distance’

Agenda

Privacy Legislation – Evolution and protection

Derogation – A non-uniform landscape

Services at a distance – Legislative changes

Privacy concerns and breaches come in all forms

Cash incentive for NHS trusts that meet targets on Liverpool Care Pathway

HOSPITALS BRIBED TO PUT PATIENTS ON PATHWAY TO DEATH

HOSPITALS are paid millions to hit targets for the number of patients who die on the Liverpool Care Pathway, the Mail can reveal.

By Steve Doughty
Social Affairs Correspondent

Your confidential medical records for sale... at just £1

Daily Mail

Daily Mail, August 2013

The INDEPENDENT

The Independent, January 2013

Patient's privacy rights shouldn't trump public safety

TORONTO SUN
torontosun.com

Toronto Sun, August 2014

With potential risk to patients

Question (which was part of 211 interviews with senior managers at 65 healthcare organisations): In your opinion, what harms do patients actually suffer if their records are lost or stolen?

Top risks to patients when their data is breached

- 61% Public exposure / Embarrassment
- 56% Financial identity theft
- 45% Medical identity theft

Source: Ponemon Institute and ID Experts, Benchmark study on Patient and Data Security, November 2010

Privacy legislation in the EU

Evolution and protection

Experience the commitment®

Europe
A large and diverse landscape

But where does privacy legislation in the European Union come from ?

Evolution 1

Adopted by the United Nations (UN) Member States and reaffirmed in 2005. The promotion and protection of human rights on a European level were inspired by this declaration. The Council of Europe was established in 1949 to promote the rule of law, human rights and democracy.

1948

Universal Declaration of Human Rights (UDHR)

The first European treaty to protect human rights. To ensure the respect of this Convention, the European Court of Human Rights was established. This Court plays a fundamental role in the application of the ECHR.

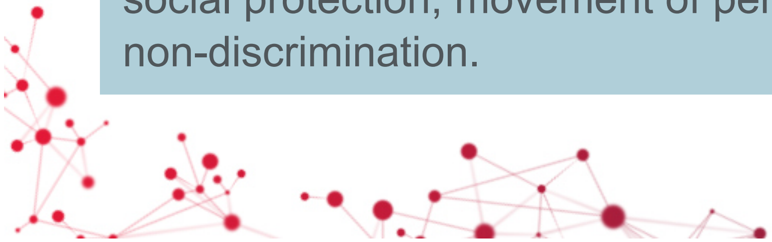
1953

European Convention for the Protection of Human Rights (ECHR)

Monitored by the European Committee of Social Rights, guarantees economic, social and cultural rights, such as the rights to housing, health, education, employment, social protection, movement of persons and non-discrimination.

1961

European Social Charter



Evolution II

The European Union Health Strategy is to ensure a high level of health protection across all policies and actions. This commitment was set out in Article 3 of the Amsterdam Treaty.

In the Treaty of Lisbon, this article serves as the most prominent legal basis for patient rights within the EU legislation, containing the first direct references to social insurance systems. This article also impressed competence on organisation and delivery of healthcare to Member States.

Another important document concerning patients rights is the ‘European Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine from 1997’, stipulating certain legal principles binding on the field of medicine and biology.

Evolution III

Article 8 of the European Convention on Human Rights:

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Evolution IV

EU Charter of Fundamental Rights:

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data 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 has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Evolution V

Data Protection Directive Article 8

(1) Member states shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

(2) Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligations of professional secrecy or by another person also subject to an equivalent obligation of secrecy

How do these relate to patient privacy? Categories of protection

General considerations

- protections, uses, and disclosures of patient information for their healthcare (Sect. 3.2)
- protections, uses, and disclosures of patient information for healthcare purposes not directly related to their healthcare (Sect. 3.3)
- obligations and justifications for the disclosure of patient identifiable information for purposes not related to their healthcare (Sect. 3.4)

The nature of consent, and the extent of the law
General considerations

Disclosure to protect interests that override the patient’s right to confidentiality (communicable disease reporting)

Carer/Guardian access to a patient’s healthcare records

Circumstances where a patient is unable to consent (adults with learning difficulties)

Patient access to a patient’s healthcare records (not all patients are the legal guardians of their own records)

Patient consent and partial consent (informed opt in/out, ‘sealed envelope’, staff members)

Disclosure after a patient’s death

Derogation

A non-uniform landscape

CGI

Experience the commitment®

How is EU legislation adopted across the EU? Overview

Although these initiatives and documents have stimulated the development of patient’s rights, EU Member States currently have no common patient’s rights legislation, varying from one country to another.

The following overview is an attempt to describe these variances by observing how the following principles vary across Member States:

- Right to informed consent
- Right to access their medical records
- Right to information concerning own health
- Right to privacy

Belgium: Law on the rights of patients, 2002

Right to informed consent	Informed consent must be given by the patient before any treatment may start. This consent only lasts as long as the medical intervention
Right to information concerning own health	The patient has the right to receive all information concerning his/her state of health .In exceptional cases, the health professional may withhold information about the patient's state of health if disclosure would cause great harm to the patient; this is called the therapeutic exception
Right to access their medical records	The patient has the right to a medical record. The law however does not give a specific definition of a medical record. Patients have the right to access their own medical records
Right to privacy	The subject of privacy is not covered in this law specifically, as this is already embedded within the Belgian Constitution. A distinction is made here between the privacy of patient data regarding health and protection, and the obligation of the physician the protection of confidence regarding the information the patient shares with the physician.

Denmark: Health Act, 2005

Right to informed consent	The act provides for the rights of patients to be included decisions made concerning their health, and including informed consent.. Minor patients (15 or over) are considered to be capable to provide informed consent.
Right to information concerning own health	Danish law does not regulate the right to information as a separate right and includes this in the overall rights of involvement of patients as described in the informed consent part of the Act.
Right to access their medical records	The act contains a provision regarding the duty of physicians to keep medical records. A provider may forward information regarding the history of the illness, cause of death etc.of a patient to relatives, when this is not considered being against the wishes of the deceased.
Right to privacy	The Danish Constitution provides the protection of privacy. The Health Act does indicate that hospitals are allowed to inform the patient's GP about treatment provided by the hospital without the explicit consent of the patient

Finland: Status and rights of patients, 1992

Right to informed consent	The patient has to give consent before medical treatments can start. If the patient refuses a certain treatment, he/she still has the right to medical care.
Right to information concerning own health	A patient shall be given information about their condition, treatment, alternative medical procedures and effects. This may include third party persons, with permission of the patient.
Right to access their medical records	Healthcare professionals shall record in patient documents the necessary information as defined in the act.
Right to privacy	Section 8 of the Constitution states that detailed provision on the protection of personal data shall be prescribed by Act of Parliament: patients must be treated in such a way that their human dignity is not violated and that their conviction and privacy are respected.

United Kingdom: No general or specific act

Right to informed consent	According to the General Medical Council the physician should seek consent before starting treatment. Also the patient should receive adequate information about the treatment.
Right to information concerning own health	This right is thus intertwined with the right to informed consent.
Right to access their medical records	This right has been laid down in the Data Protection Act of 1998. Patients have the right to access their medical record at all times.
Right to privacy	Common Law covers the relationship regarding doctors and patients and the need for confidentiality. The doctors are obligated to respect the confidentiality of the patients. The Common Law however does not cover the right on privacy, which is protected by the Data Protection Act.

Services at a distance

Legislative difficulties

CGI

Experience the commitment®

What is eHealth?

A broad definition:

- The interaction between patients and healthcare providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and / or health professionals through information and communication technologies.

Examples include:

- HIEs, electronic health records, telemedicine services, wearable and portable systems that communicate health information, and many other things too numerous to mention

eHealth and the rise of new demands

But e-health also enables service providers from different EU member states to work more closely together. If a particular treatment can be provided to a patient more effectively in another country, e-health systems make it simpler to organise and carry out treatment abroad.

However…. New demands are being placed on the existing regulatory frameworks.

Telemedecine

Teleconsulting

Regulatory Frameworks

Telepathology

Teleradiology

Disruptive technologies, such as social media, and how they can be harnessed to facilitate more effective disease management through patient networks, will stress these frameworks in ways we can only vaguely anticipate today.

Telemedecine

- Telemedicine is both a health service and an information society service
- Health services are generally governed at the member state level
- However, the EU electronic Commerce Directive 2000/31/ EC (E-commerce Directive) provides the legal framework for information society services, which include any service normally provided or remuneration, at a distance, by electronic means and at the individual request of a recipient of services

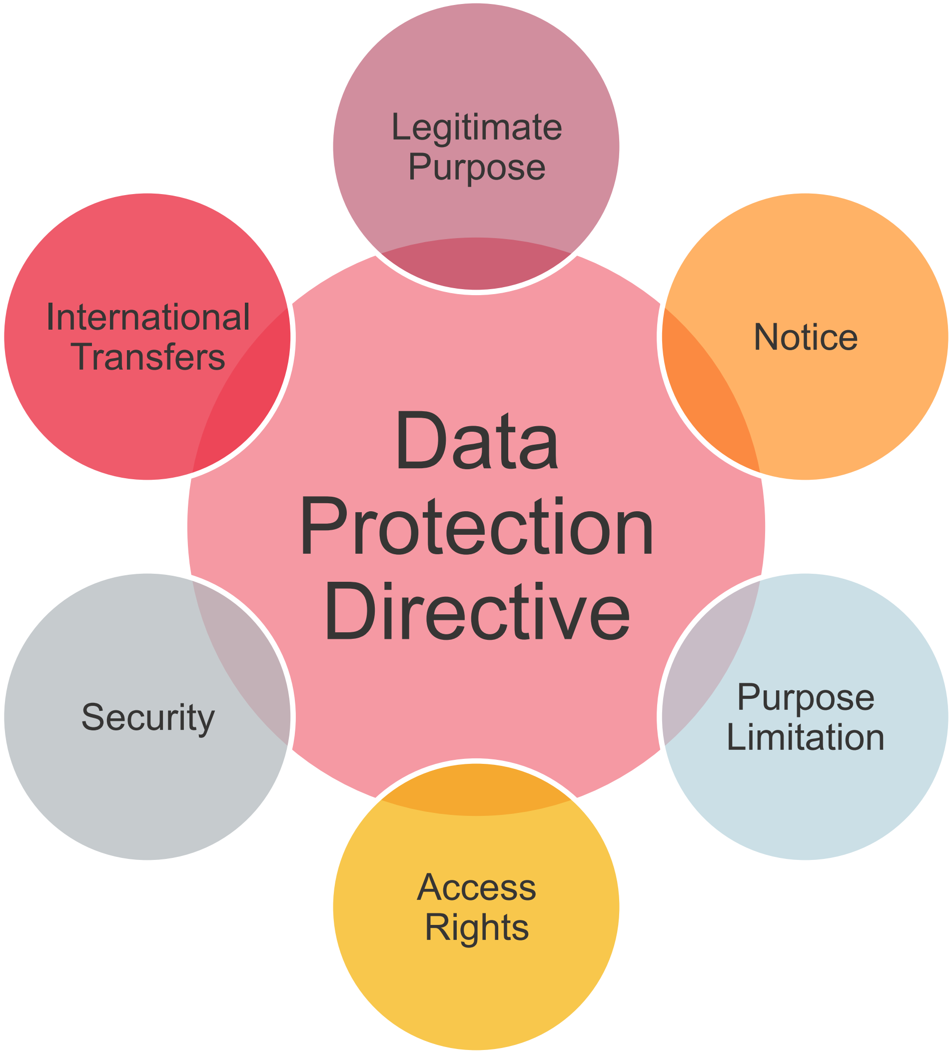
Defining “at a distance”

A service is provided without the parties being in the same place at the same time

Service at a distance

Legislative challenges:

E-health operators are expected to comply with member state laws implementing the Data Protection Directive, of which the most notable obligations are illustrated



Legitimate Purpose

Notice

Purpose Limitation

Access Rights

Security

International Transfers

Data Protection Directive

Legitimate Purpose

Legitimate Purpose

Use case

Data processing is permitted if it is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional bound under national rules to the obligation of professional secrecy

Challenges

- Patient support networks, generally associated with a chronic condition, where patients assist each other through emotional support and advice
- Rehabilitation through Gaming Theory, particularly among the injured service personnel in civilian life

Notice

Notice

Use case

Patients should be given information about

- the purposes for which their health information will be processed
- disclosures of information to third parties (eg, other healthcare professionals responsible for managing the patient)
- any transfers of personal information outside the EU, particularly disclosures to operations in the US

Challenges

- Information for Secondary Purposes; impossible to declare what reasons the data will be used for
- Increasing collaboration between health and social care
- Large scale sequencing programmes, where small-cell anonymisation can't be guaranteed

Purpose Limitation

Purpose
Limitation

Use case

Personal and health information collected via e-health systems should only be processed for the purpose of providing the e-health services and should not be processed for any other purpose not disclosed to patients using the service. In particular, health information should not be sold or commercialised in any way without first informing individuals

Challenges

- Commercial value of healthcare data to the pharmaceutical sector shouldn’t be underestimated

Access Rights

Access
Rights

Use case

Under the Data Protection Directive, individuals have the right to request a copy of any personal information processed about them, a principle embodied in the new cross-border healthcare directive

Challenges

- All data? Very difficult in a connected world – the list of obvious challenges is long, but how to manage data such as:
  - Mental health diagnoses
  - Sexual health histories
- For older citizens who grant authorisation to their informal carers

Security

Security

Use case

While imposing a general security requirement, the Data Protection Directive does not mandate particular security measures for data at rest or in transit. Different EU member states often have their own security requirements that must be complied with. In the transfer context, there is a strong preference for applying reliable encryption techniques to data transfer

Challenges

- Current legislation is exclusively provider-centric.
  - How do we address citizens accessing their health records from their own devices?
  - How do we securely identify our citizens and their nominated carers?

International Transfers

International Transfers

Use case

For transmission outside the EU, e-health operators need to comply with European restrictions on cross-border data transfers. However, some EU member states preclude the actual transfer of certain types of patient data (UK NHS electronic medical records, for instance) from outside their jurisdictions, making international processing of patient data outside the EU difficult. For example, contracts let by the NHS, preclude the transfer of patient information outside the UK.

Challenges

- The world is running short of radiologists, pathologists and certain other clinical disciplines. Demand increases, supply decreases or remains fixed, and cost and quality suffer. Technology enabling the delivery of services at a distance from elsewhere in our connected world will allow us to drive innovation into healthcare to reduce cost and improve quality.

In Summary: technological disruption

Ours is the last of the great supply-driven industries. The major transformational forces facing us over the next decade will be disruptive.

Legislation is always behind technology, but as these disruptions transform our healthcare landscape, we need legislative frameworks that are adaptable and agile to accommodate the great changes we will observe.

Questions

CGI

Experience the commitment®

Innovative solutions. Smarter decisions. Better outcomes

Experience the commitment®