AEMH - Data protection
Data protection in the context of medical files
May 2017
Human dignity
Human dignity is inviolable. It must be respected and protected.

Right to life
Everyone has the right to life. No one shall be condemned to the death penalty, or executed.

Right to the integrity of the person
Everyone has the right to respect for his or her physical and mental integrity...

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

Data Protection
Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes...
Data protection and other fundamental rights
Handling the conflicts

• Fundamental rights can be conflicting
  − Either for a same person
  − Or for different persons

• There is no right more important than the other

• A fair balance must be struck

• The necessity must be appreciated
How to protect medical files

- Designate a Data Protection Officer
- Assess the need of a Data Protection Impact Assessment and go through with it and document it
- Implement strategies like Data Protection by design and by default

Medical files

- The GDPR defines health data as a special category of data
- All Member States have specific local legislation handling health data, patient records and professional secrecy in the medical sector
- Automated decision making is limited (consent, public interest)
Data Protection Impact Assessment
What it is and what it should include

01 A systematic description of the envisaged processing operations and the purposes of the processing

02 An assessment of the necessity and proportionality of the processing operations in relation to the purposes

03 An assessment of the risks to the rights and freedoms of data subjects

04 The measures envisaged to address the risks, including safeguards, security measures ...
Security measures
How to secure the access in a medical environment

- Anonymization or pseudonimization of data as a measure to avoid disclosure
- Use of Biometrics to secure access without physical contact i.e. Iris scans are highly reliable and very quick
- Encryption of data wherever achievable
- Use RFPs to choose the right vendor with a high level of security and data protection awareness
Creating Awareness
Awareness of the risks and available safeguards is the first line of defence

- Awareness Trainings
- Simulated Phishing attacks
Contact

Georges Wantz
Director
Technology & Enterprise Application
gwantz@deloitte.lu
+352 451 454 363
Deloitte is a multidisciplinary service organization which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 225,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.