E-health: ethical and data privacy challenges in the EU

Brian Kelly

E-health is a relatively new area of medical technology, and there is a need for clearer EU regulations governing its use. Brian Kelly, an associate in the Life Science Practice of UK law firm Covington & Burling, considers the regulatory framework for e-health, with a focus on the ethical and data privacy challenges

E-health covers 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 health information networks, electronic health records, telemedicine services, wearable and portable systems that communicate health portals, and many other software-based tools that help disease prevention, diagnosis, treatment, health monitoring and lifestyle management. E-health also enables health 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, the wider deployment of e-health, in particular in telemedicine and telemonitoring, raises new ethical and regulatory concerns. The lack of a clear regulatory framework for e-health products and services coupled with the need to ensure patient health information remains private and secure needs to be addressed to build trust and confidence in e-health systems.

Regulatory framework

Health and information society services

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 for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. "At a distance" means that the service is provided without the parties being in the same place at the same time. Services that are carved out of the E-commerce Directive include medical examinations or treatment at a doctor's surgery using electronic equipment where the patient is physically present; and services that are not provided via electronic processing/inventory systems, including a "telephone/telefax consultation of a doctor".

Medical devices

E-health products used for a medical purpose may fall under the definition of a medical device under the Medical Device Directive 93/42/EEC, as amended (MDD). Medical devices include software, instruments and appliances, including software intended to be used specifically for diagnostic and/or therapeutic purposes, and software necessary for a device's proper applicationin diagnosis, prevention, monitoring, treatment or alleviation of disease.

E-health products that could fall under this definition include wireless monitoring devices for recording blood pressure, picture archiving and communications systems, and devices for calculation of anatomical sites of the body.

The European Commission has historically viewed software used for administration of general patient data – medical records, bookings and appointments – as being outside the scope of the MDD. However, a number of national regulators have revisited the issue of the borderline area between software and medical devices following amendments to the MDD that came into force in March 2010 and placed greater emphasis on use of software.

Data protection and confidentiality

E-health products and services are most likely to involve the processing of patient health information. The processing of such sensitive personal information is governed at the EU level under the Data Protection Directive 95/46/EC, as amended (Data Protection Directive) and the E-Privacy Directive 2002/58/EC, as amended (E-Privacy Directive). These directives lay down specific requirements to safeguard an individual's rights to privacy and to ensure that communications and networks are secure. Indeed, the recently adopted directive on patients' rights in cross-border healthcare makes clear that providers of cross-border e-health must comply with the Data Protection Directive.

In addition, EU member states have their own laws, regulations and guidance governing the processing of health information. For example, the Department of Health in the UK requires all e-health operators working within or for the National Health Service (NHS) to comply with the Department of Health's Confidentiality Code of Practice and Guidelines on Information Security, which can require higher standards than those under EU law. These codes and guidelines make clear that telemedicine consultations, emails and pictures sent electronically are likely to form part of a patient's medical record, which would trigger separate rules governing record retention.

Restrictions and requirements under the Data Protection Directive

E-health operators are expected to comply with member state laws implementing the Data Protection Directive (ie under the UK Data Protection Act 1998). The most notable obligations are as follows:

- Legitimate purpose: Identifiable health information may only be processed if at least one of several conditions appearing in Article 8 of the Data Protection Directive is satisfied. For example, 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. Processing may also take place if the patient has given explicit consent or if it is necessary to protect the vital interests of the patient (usually life or death situations).
- Notice: In addition to the above, patients should be given information about the following, among other things: (i) the purposes for which their health information will be processed (eg, for diagnosis); (ii) disclosures of information to third parties (eg, other healthcare professionals responsible for managing the patient); and (iii) any transfers of personal information outside the EU, particularly disclosures to operations in the US (eg, if the data are stored on a US server or are accessed by maintenance operators based in the US). This information is necessary to satisfy the requirement of fair and lawful processing under the Data Protection Directive.
- Purpose limitation: Personal and health information collected via e-health systems should only be processed for the purpose of providing the e-health services (or other related purposes disclosed to patients) 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 of this use of their personal and health information and obtaining their prior consent.
- Access rights: 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.
- Security: The Data Protection Directive specifies that appropriate technical and organisational measures be taken against unauthorised or unlawful processing of personal data and to protect personal data against accidental or unlawful loss, damage or destruction. While imposing a general security requirement, the Data Protection Directive does not mandate particular security measures for data at rest or in transit. As noted above, however, 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 transferred over electronic networks and pathways. Patients should be informed, however, that no method of transmitting or storing electronic data is ever completely secure. When transmitting data electronically, e-health operators should therefore apply the "postcard test", ie, if you are uncomfortable sending particular information by postcard then sending this same information by email could also be problematic.
- International Transfers: To the extent that personal or health information is transmitted or accessible to persons outside the European Economic Area (EEA), then e-health operators would need to comply with European restrictions on cross-border data transfers. This may entail the use of data transfer contracts executed between the operator and parties located outside the EEA or obtaining the unambiguous consent of the patient to transfer their data to such foreign jurisdictions. However, some EEA 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 hosting of patient data outside the EEA difficult in some cases. For example, according to the UK Department of Health, contracts let by the NHS Connecting for Health agency, which is responsible for delivering the UK national IT programme, preclude the transfer of patient information outside the UK.
- Notification: e-health operators generally would need to notify the regulatory authority where the operator is based of their processing of personal data to (so e-health providers in the UK that process personal data would need to file a notification with the UK Information Commissioner's Office). It is possible that in some countries operators may benefit from an exemption.

Doctor-patient relationship

The increasing use of telemedicine as a replacement for physical face-to-face consultations is becoming more acceptable provided patients are offered a physical examination where appropriate and patient privacy is safeguarded as described above. Indeed, some member states require healthcare professionals to offer a physical where appropriate; for instance, section 15 of the UK National Health Service (General Medical Service Contracts) Regulations 2004 states that doctors must be contractually obliged to offer NHS patients a physical examination where appropriate.

However, the use of cross-border e-health services raises additional concerns. For example, professional medical and ethical standards are not harmonised at the EU level, meaning that a doctor in one member state may be practising at a different professional and ethical standard to a doctor in another member state. There are also concerns over patient access to redress if treatment goes wrong and the conflict of jurisdiction issues that flow from cross-border treatment. The newly-adopted directive on cross-border healthcare hopes to address some of these issues.

E-health has huge potential to improve patient care but there are a number of regulatory and ethical challenges that need to be dealt with to increase patient and user confidence in the technologies. One of the fundamental challenges is ensuring that patient data remain confidential and secure. The Data Protection Directive provides a binding EU framework to safeguard patient privacy, and e-health operators should systematically assess the data privacy aspects whenever e-health services are provided. However, e-health operators need to be mindful of and compliant with national laws and regulations governing the specific processing of patient health information, which can require higher standards.

** Brian Kelly can be contacted at bkelly@cov.com*