PGEU GPUE
Pharmaceutical Group of European Union
Groupement Pharmaceutique de l'Union Européenne

CED
COUNCIL OF EUROPEAN DENTISTS

CPME
COMITÉ PERMANENT DES MÉDECINS EUROPÉENS
STANDING COMMITTEE OF EUROPEAN DOCTORS

EPF
European Patients Forum

EFN

Consensus Framework on the Digital Transformation of Healthcare

In this Consensus Framework CED, CPME, EFN, EPF and PGEU outline joint key recommendations for the digital transformation of healthcare in support of high-quality patient care. This Consensus Framework neither aims to be comprehensive nor does it constitute a single common policy of the organisations involved. The individual CED, CPME, EFN, EPF and PGEU policies outlined in the resources section set out each organisation's detailed commitments and offer more diverse and in-depth information and guidance.

Preamble

Digital technologies and their applications to the health sector are quickly expanding. Governments increasingly adopt the use of digital technologies in the health sector, thereby exploring the use of data for decision-making and considering new solutions to strengthen their health systems.[1] However, without an appropriate and enforceable legal framework, digital technologies can open the door to illegal practices and abuse thereby endangering patient safety or hampering patients' rights. This threat has been exacerbated during the COVID-19 pandemic, which has resulted in a substantial increase in the use of digital health services and online provision of healthcare products. A number of investigations conducted by various national authorities illustrate the vulnerability of consumers vis-à-vis the unlawful supply of coronavirus-related products by online platforms[2].

CED, CPME, EFN, EPF and PGEU acknowledge the value of digital innovation in bringing benefits for citizens, patients and health systems. We believe digitalisation can support healthcare professionals in delivering high quality health and care services. Doctors, nurses, dentists and community pharmacists use digital technologies daily, for instance, when issuing or dispensing electronic prescriptions, accessing electronic health and medication records, checking for medication interactions, or providing support via a mobile app or telehealth. They also collect and generate real world evidence that can contribute to evidence-based health policy and best practices in patient care. Digital tools can also empower patients to become more actively involved in their own healthcare and to enhance communication with healthcare professionals.

CED, CPME, EFN, EPF and PGEU welcome the proposal to create a European Health Data Space (EHDS) as an opportunity to promote the sharing of health data[3] across borders to enable more personalised diagnoses, advice, and innovative medical treatments. Sharing health data needs to go along with strong legal safeguards and security as well. Inclusive governance structures and transparency are essential to supervise the use and re-use of health data. CED, CPME, EFN, EPF and PGEU also recognise the potential of Big Data and Artificial Intelligence (AI) for European health systems and consider these technologies as a useful tool to support professional practice.

[1] WHO | New ethical challenges of digital technologies, machine learning and artificial intelligence in public health: a call for papers.

[2] See PGEU collection of examples of illegal conduct regarding the online supply of medicines

[3] For the purposes of the Consensus Framework 'health data' are understood as 'data concerning health' within the meaning of Art. 4 (15) GDPR: "data concerning health" means *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"*.

Healthcare professionals remain a trusted source of reliable and independent health information for patients. They have ethical and legal obligations to protect sensitive personal data. This includes privacy and confidentiality obligations. Doctors, nurses, dentists and community pharmacists are key to bridge patients and health systems and ensure patients are well informed on how their healthcare data is used to improve the safety and quality of their treatment. The patient perspective is essential to ensure that tools are co-developed with patients and add value for them. Healthcare professionals and patients are therefore the key reference in the formulation of EU policies on digital technologies in health. It is our view that when considering the impact of any proposed measures at EU level affecting health, economic objectives should not prevail over quality of care, access to care and patient safety.

*The **Council of European Dentists** (CED) is a European not-for-profit association representing over 340,000 dental practitioners across Europe through 32 national dental associations and chambers in 30 European countries.*

*The **Standing Committee of European Doctors** (CPME) represents 38 national medical associations across Europe, giving voice to over 1.6 million doctors.*

*The **European Federation of Nurses** Associations (EFN), represents 36 National Nurses Associations at European Level and its interests to the European Institutions.*

*The **European Patients' Forum** (EPF) is an organisation counting 77 members representing patient organisations across Europe and across disease-areas.*

*The **Pharmaceutical Group of the European Union** (PGEU) is the association representing 400,000 community pharmacists in 32 European countries.*

Our Key recommendations

1. Digital Health – Citizens' Trust is Key

- Guarantee a high level of data protection and full compliance with professional ethics in digital health.[4] It can be expected that the adoption of big data and related analytics technologies in healthcare will challenge governance, quality, safety, standards, privacy and data ownership. To keep trust, it will be essential that the collection of health data will be done in compliance with the General Data Protection Regulation ('GDPR)', the future EU regulatory framework for AI[5] as well as professional ethics.
- Include health professionals' advice, alongside patients' views in the design and validation of digital health (policies, services and technologies) to improve workflow efficiency, while promoting treatment effectiveness and offering the highest quality of healthcare to patients. Co-creating digital health, from policies to technological innovation, should be embedded as a core principle 'by design'.
- Develop clear standards and legally binding assessment criteria to ensure transparency of AI systems in healthcare. Transparent, clinically validated AI and systematic quality checks could foster the acceptance and trust among the users of AI systems. This should be coupled with clear liability mechanisms, offering adequate protection in case of errors or misuse of AI in healthcare.
- Offer training on AI techniques and approaches (e.g. machine learning), initiating at the undergraduate level, which must be supported by appropriate structures in the practicing environment. The workforce needs to be appropriately trained and financially supported during the introduction and application of AI systems in healthcare settings.
- Design and implement more targeted and effective policies and initiatives aimed at improving digital health (and data) literacy for citizens and patients. Increased awareness and understanding of digital health and health data is instrumental in building trust and enable better and safer exploitation of digital health services and innovation, in particular by less health/digital literate people.
- Communicate and collaborate among patients, health professionals and ICT developers to realise the full potential of digital health systems. When developing guidelines, policy makers are called upon to meaningfully involve and consult their users. Systems facilitating the

[4] Digital health is a broad umbrella term that refers to "the use of information and communication technologies in medicine and other health professions to manage illnesses and health risks and to promote wellness [https://www.ncbi.nlm.nih.gov/books/NBK470260/]." According to the World Health Organization (WHO), the term encompasses electronic health (eHealth) and developing areas such as "big data", genomics and artificial intelligence to strengthen health systems and public health, increase equity in access to health services and work towards universal health coverage [https://www.euro.who.int/en/health-topics/Health-systems/digital-health.]. This definition also includes telehealth, telemedicine and mobile health (mHealth).

[5] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

identification of trustworthy and secure digital health solutions (e.g., labeling) should also be considered as a tool to improve trust and foster information.

2. Health Data Sharing – Patient Autonomy and Confidentiality are Key

- Respect human dignity and other fundamental rights when sharing health data. Following the principle of patient autonomy, the patient has the right to self-determination, to make free decisions regarding himself/herself. The patient has the right to give or withhold consent not only to any diagnostic procedure or therapy but also before disclosing health data to third parties, e.g., researchers, governments, or insurance companies – unless there is an appropriate lawful justification in line with GDPR rules.
- Do not discriminate because of people's genome. The use of genetic data for insurance, banking, criminal justice, education or employment purposes must never be allowed.
- Inform patients as to who will have access to his or her health record when obtaining consent to share health data, ensuring that health data is used in a manner which is scientifically sound and ethically acceptable. Transparency and security procedures in relation to access to data are of paramount importance.
- Ensure patients full control and visibility on their electronic health records, also in order to verify their correctness in constant dialogue with healthcare professionals.
- Consider risk mitigation and health literacy in relation to privacy and professional confidentiality as many health data are exposed in online platforms, social media and apps.
- Enable ePrescriptions at national level and in cross-border settings. Make the system user-friendly and integrated in a shared electronic health records (EHR) system, allowing health professionals to access necessary patient information. The system should also be designed to avoid potential gaps in access to information for patients.

3. Online Provision of Medicines - Patient Safety and Patients' Rights are Key

- Use online provision of medicines only to complement face-to-face interactions between health professionals and patients. Online provision of medicines does not replace personal interaction and patient-health professional relationships, which must continue thriving and bringing benefits to local populations.
- Follow the same fundamental ethical principles and adhere to the same professional standards in online dispensing of medicines as with face-to-face dispensing. A level playing field between online platforms and traditional offline providers should be granted. Commercial platforms may not always be fit for purpose nor be fully compliant with EU data protection law or be easily integrated into existing electronic health records. Moreover, the digital solutions offered may not always be driven by improvements to quality of care.[6]
- Declare any conflicts of interest. The online provision of medicines should be operated by health professionals with the aim to improve quality of care and not by commercial motivations.
- Guarantee patient safety and quality of care according to the level of protection determined by the country where the patient is established. Patients must be able to rely on the fact that the dispensing rules as well as quality and safety standards of their home country are respected regardless the offline or online form used to acquire their medicines.
- Introduce effective cooperation and enforcement procedures for cross-border issues in EU law while ensuring a proper oversight over online provision of medicines.
- Strengthen the responsibility of online providers of medicines and online platforms making available medicines: e.g. increase awareness of the EU logo identifying legitimate internet sellers of medicines, active prosecution of marketplaces that do not respect regulations and legal requirements by competent authorities.
- Improve the enforcement of EU and national rules protecting patients and public health by ensuring illegal practices are swiftly detected, stopped and sanctioned - what is illegal offline should also be illegal online.

[6] An example of this threat is an undergoing investigation launched in July 2020 by the Polish data protection authority as a result of a complaint lodged by the Polish Ministry of Health regarding illegal access by a big online marketplace to e-prescription records through the public authority database. If confirmed, this practice would have enabled such an online platform to profile patients based on such sensitive data with mere commercial purposes. See official press release here.

4. Telemedicine and Telehealth Services - Patient Safety and Patients' Rights are Key

- Use telemedicine and wider telehealth services to complement face-to-face consultations. Telemedicine and telehealth can be a useful tool in certain clinical scenarios, such as improving access to medical and other healthcare professionals expertise or where distance to services and patient mobility are an issue. Telemedicine and telehealth services cannot replace personal interaction and physical examination by health professionals.
- Follow the same fundamental ethical principles and adhere to the same professional standards in teleconsultations as with face-to-face consultations.
- Do not allow commercial factors to influence telemedicine and telehealth services. Commercial platforms may not always be fit for purpose nor be fully compliant with EU data protection law or be easily integrated into existing electronic health records. Moreover, the digital solutions offered may not always be driven by improvements to quality of care.[7]
- Do not use telemedicine and telehealth services as a cost-saving measure to justify the closure of healthcare facilities, especially in less populated areas. Telemedicine and telehealth services should be operated by clinicians with the aim to improve the quality of care and not by commercial motivations – any conflicts of interest should be clearly declared.
- Set up secure and stable platforms that protect patient confidentiality. Telemedicine and telehealth services that improve patient safety, quality of care and efficiency must be supported with government investment and services appropriately reimbursed as part of a health services catalogue.
- Embed co-production with patients and healthcare professionals in the development and adoption of telemedicine and telehealth services and related policies. The full potential of telemedicine and telehealth services will only be realised if they truly answer patients and healthcare professionals' needs.
- Telemedicine and telehealth should be always deployed keeping in mind needs and accessibility for citizens and patients. Potential challenges such as health literacy gaps, technical access to digital solutions or platforms should be considered, to avoid one-size-fits-all approaches that would potentially exacerbate inequalities. Dedicated information/health literacy activities should be considered to support equal safe and informed use of telemedicine and telehealth.

[7] Ibid.

- Appropriately strengthen health professionals' digital skills and support them with clear guidance relevant to their specialty.

Resources

CED

- *CED Resolution on Artificial Intelligence in Dentistry, November 2020*
- *CED Resolution on Dental Data Set and Access to Health Records, November 2019*
- *CED Resolution on Data Sharing as part of eHealth, November 2018*
- *CED Resolution on eHealth, November 2012*

CPME

- *CPME Policy on the European Health Data Space – Focus on Health Research and Policy Making, March 2021*
- *CPME Policy on Telemedicine, March 2021*
- *CPME Policy on Digital Competencies for Doctors, November 2020*
- *CPME Statement on Online Advertising of Unhealthy Products for the Digital Services Act Public Consultation, September 2020*
- *CPME Policy on AI in Health Care, November 2019*
- *CPME endorses the WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks, April 2017*
- *CPME Policy on mobile health, October 2015*

EFN

- *EFN Position Statement on Nurses Co-Designing Artificial Intelligence Tools, April 2021*
- *EFN Policy Statement on Nurses Digital Competencies, November 2019*
- *EFN Policy Statement on End-User Co-Designing EU Digital Health Systems, October 2019*
- *EFN Position Paper* on Public Health Virtual Coaching*, March 2017*
- EFN *Position Paper on Robotics in Nursing, March 2017*
- *EFN Report on Digitalisation (EFN European Parliament Event 05/02/2020), February 2020*
- *eHealth Stakeholder Group report on 'eSkills and Health workforce', November 2014*
- *Leveraging the trust of nurses to advance a digital agenda in Europe: a critical review of health policy literature (By Paul De Raeve, at Al, Open Research Europe, May 2021)*
- *Digitalising the healthcare ecosystem in the European Union (Paul De Raeve, Ricardo Jardim-Gonçalves, Health Europa Quarterly – Issue 13, May 2020, pp14-17)*
- *The world of cloud-based services: storing health data in the cloud (By Paul De Raeve, Health Europa, August 2019)*
- *Three million EU nurses leading digitalisation! (By EFN, Open Access Government, December 2017)*
- *EFN response to the EC consultation on the European Health Data Space (EHDS) (May 2021)*
- *EFN response to the EC consultation on the European health data space inception impact assessment (January 2021)*

- *EFN response to the EC Consultation on the White Paper on Artificial Intelligence – A European Approach (April 2020)*
- *EFN response to the EC Consultation on Transformation Health & Care in the Digital Single Market (August 2017)*
- *EFN response to the EC Consultation on eHealth Action Plan 2011-2020 (May 2011)*

EPF

- *EPF response to EC European Health Data Space Feedback Consultation, February 2021*
- *EPF response to EC Data Governance Act Feedback Consultation, February 2021*
- *EPF response to EC Data Strategy Consultation, June 2020*
- *EPF response to EC Artificial Intelligence White Paper, June 2020*
- *EPF Briefing Paper on AI and Big Data, May 2020*
- *EPF Policy page on Digital Health and Data Protection (including EPF GDPR Papers)*

PGEU

- *PGEU Position paper on the Digital Services Act, September 2020*
- *PGEU collection of examples of illegal conduct regarding the online supply of medicines, March 2021*
- *PGEU response to EC Roadmap on Artificial Intelligence, August 2020*
- *PGEU paper on Big Data and Artificial Intelligence in healthcare, February 2019*
- *PGEU feedback on the EC roadmap on the European Health Data Space, February 2021*
- *PGEU position paper on digital health, June 2021*