The Consumer Voice in Europe

DIGITAL HEALTH

PRINCIPLES AND RECOMMENDATIONS

Contact: Jelena Malinina – health@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2018-090 - 15/10/2018

Why it matters to consumers

Health and healthcare services are rapidly and inevitably changing due to new technologies. Traditional health is becoming digital. Consumers will be profoundly impacted by the ongoing and future developments in healthcare services. On the positive side, digitalisation of health care has a potential to deliver better disease prevention, diagnosis and treatment. Tools such as the electronic health record (EHR) may allow consumers 24/7 access to their disease history and medicines prescriptions, also when travelling or moving abroad. Mobile health (m-health) apps and online doctor consultations may provide an excellent support for patients and consumers in their efforts to maintain their health and prevent diseases. However, the benefits of digital health products and services come together with high risks when it comes to consumer privacy, security and safety. With health data becoming a new currency, security breaches of personal health records and data stored in the healthcare settings may become more frequent. The questions of trustworthiness and safety of digital health products and services are also potent.

Summary

KEY DIGITAL HEALTH PRINCIPLES

To ensure that digital health products and services are safe, beneficial and trustworthy for all European consumers, the following key digital health principles must be observed and respected:

1. **Consumers must have full control over their personal health data**. Consumers must have a right to decide on how and with whom to share their data, they must also be able to access their health data and report on possible errors anywhere and anytime.
2. **Health and medical data of consumers must be accurate and up-to-date**; mechanisms to correct medical errors must be enabled.
3. Consumers must benefit from **digital health tools which respect privacy and security by design and by default principles.**
4. **Digital health products and services must be safe and reliable to use.**
5. **Digital health products and services must be closely supervised by the competent authorities.** In case any safety, security or privacy concerns are suspected or detected, the authorities should intervene swiftly and take necessary measures.
6. Digital health solutions should be promoted only along with **access to an affordable, high-quality, high-speed internet connection for all** to enable safety and accessibility of such solutions.
7. Consumers have different needs, capacities, values and goals when it comes to their use of digital health tools. **Digital health products and services must correspond to the variety of users' preferences, also respecting a preference not to use a digital health product or service**. The **level of digital health literacy should also be improved** both among consumers and healthcare professionals.

KEY DIGITAL HEALTH REGULATORY RECOMMENDATIONS

We recommend that

1. The **General Data Protection Regulation (GDPR) must be diligently implemented across the EU.** The **balance between the interests of scientific health research and consumers' protection can be achieved** through an adequate use of the GDPR exceptions and special provisions regarding scientific research.
2. **Artificial intelligence in healthcare must be applied in full respect of EU data protection rules,** considering the principles of fairness, transparency, purpose limitation, data minimisation, accountability and privacy by design. **Automated processes based on algorithms must be transparent to consumers and discrimination avoided.**
3. **In the context of the Medical Devices Regulation's provisions on IT security, the EU should ensure that it is implemented in full respect of the principle of security by design and by default.** Further details should be provided on what is considered a minimum standard and how manufacturers should ensure it.
4. **A minimum set of security measures must be obligatory for all digital health connected products**, including health and well-being apps as a condition for putting them on the market.
5. The **Security of digital medical systems in healthcare settings must be strengthened** through the timely and diligent transposition and implementation of the NIS Directive.
6. **The Radio Equipment Directive and the General Product Safety Directive must be updated to cover safety issues of digital health connected products falling outside of the scope of the Medical Devices Regulation**.
7. The EU should **develop a comprehensive regulatory framework** to ensure a harmonised approach and high privacy and security standards of lifestyle and well-being apps.
8. Given a growing use of digital health services and products, also in cross-border environment, it is of key importance to **harmonise the approach to the liability of such services and products across the EU.**
9. Legislative measures such as **strong market surveillance, law enforcement, as well as efficient redress** tools on digital health products and services must be put in place to contribute to an effective protection of EU consumers.

BEUC The European Consumer Organisation

Contents

Introduction

Digital health products and services are everywhere: we use health apps on our smartphones, health records are increasingly digital, and our blood values are shared with our doctor via the internet. With health and care digitalisation being on top of the EU's public health policy agenda, it is expected that in the upcoming years more and more governments will be implementing digital solutions into their healthcare systems and boosting digital health across the EU.

In 2018, the European Union committed to the following priorities on digital health:[1]

1. Enabling citizens to access their health data across the EU;
2. Allowing researchers and health professionals to share data, expertise, computing processing and storage capacities across the EU;
3. Using digital tools to empower people to look after their health, stimulate prevention and enable feedback and interaction between users and healthcare providers.

Financial support for implementation of the outlined priorities is foreseen in the new European Multiannual Financial Framework 2021-2027. BEUC welcomes this development. However, it is important to ensure that digitalisation actually leads to increased consumer welfare and well-being.[2]

While digital health holds a lot of potential, it also has a lot of unresolved issues when it comes to privacy, security and safety. They are also often made without a focus on what users really need. Furthermore, the consequences of health digitalisation are not limited only to greater use of mobile health apps or implementation of the European electronic health record systems, its effect is reaching further than that. Digital health solutions produce enormous amount of health data about its users, which can be used to extract previously unknown information about human health and diseases. The analysis of these large data sets is called data mining and serves as a foundation for artificial intelligence and machine learning which can truly transform the way diseases are prevented, treated and diagnosed. However, to fully benefit from these advancements it is of key importance to first implement digital health elements with a high consideration of data privacy, security, accuracy and inclusion of consumer needs.

There is no room for mistake when it comes to management of consumer sensitive data. Given the critical time of the European health digitalisation, in this paper BEUC aims to establish key digital health principles and regulatory recommendations to be considered when establishing digital health products and services.

[1] European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market, April 2018, https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

[2] BEUC Position Paper, The New Multiannual Financial Programme 2021-2027, March 2018, http://www.beuc.eu/publications/beuc-x-2018-015_the_new_multiannual_financial_framework.pdf

1. Privacy and data protection in Health - From Hippocrates to the GDPR

A patient's right to privacy and confidentiality of their health is as old as the science of medicine. The obligation of physicians to protect the privacy of their patients was enshrined in the Oath of Hippocrates, dating back to the fourth century BC: *"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account must be spread abroad, I will keep to myself…."*[3] Undoubtedly, both medicine and patient-doctor relationship have changed since the Hippocrates time, but the question of patients' privacy is as important as ever.

Nowadays the importance of protecting patients' health data and privacy is emphasised due to increased electronic health data processing happening though the use of various digital health products and services. In the upcoming years the amount of digitalised health information is going to increase with the use of electronic health records (EHR). EHR is a broad term but overall it is aimed to enable users to access their medical history data; allow electronic medicine prescriptions and dispensing; facilitate digital storage of laboratory data etc. EHR can help with reducing medical errors, enable better documentation and provide patients with access to their medical record any time.

For European consumers to enjoy the benefits of digital health solutions it is of key importance to create the necessary tools to guarantee the protection of their data and privacy. The General Data Protection Regulation (GDPR) is the EU's main legal instrument to protect individuals, laying down important provisions on health data processing.

Almost all EU Member States have implemented certain elements of the EHR into their healthcare systems, some of them have fully functional national EHR models, others are on the way to develop one.[4] While the status of national EHRs varies, the idea to develop the EU-wide EHR system was enshrined into the European Cross-Border Healthcare Directive[5] in 2011 and confirmed in the European Commission's recent Communication on digital health[6] (2018). The European EHR system would allow European citizens to share their electronic health records across countries when travelling or moving abroad. BEUC welcomes the creation of the EU system to exchange EHR, however, urges the European Commission to make sure that the operational design of the system ensures consumers are in control of their personal data and the GDPR provisions on health data processing are adequately implemented.

---

3 Rothstein MA. The Hippocratic Bargain and Health Information Technology. The Journal of law, medicine & ethics: a journal of the American Society of Law, Medicine & Ethics. 2010;38(1):7-13.

4 European Commission, Staff Working Document on enabling the digital transformation of health and care in the Digital Single Market, April 2018 https://ec.europa.eu/digital-single-market/en/news/staff-working-document-enabling-digital-transformation-health-and-care-digital-single-market

5 Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, March 2011, https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024

6 European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market, April 2018, https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

1.1. Consumer control over their personal health data

Consumers must have full control over their personal health data. Consumers must have a right to decide on how and with whom to share their data, they must also be able to access their health data and report on possible errors anywhere and anytime.

With the wider use of digital technology in healthcare, it is of key importance to ensure that consumers are informed on how their personal health data is used and have full control over it. Health data can provide a lot of valuable information about a person, or overall lifestyle and diseases of particular population. BEUC's Norwegian member Forbrukerrådet performed a test of several health and well-being (fitness) wearables, and all tested devices collected more data than necessary to deliver the service, and none of them explained with whom the collected data was shared. Similar discoveries were made when analysing connecting blood pressure devices and blood sugar monitors. For example, the app connected to one device was transmitting user data to a server in China, without any information given to the user, and without the user's consent.[7]

The Portuguese Consumer organisation DECO found that several tested fitness watches and bracelets had no obvious way to reset and there is a concern that this could leave users data vulnerable if they give or sell their tracker to another person.[8]

Such situations are unacceptable and the GDPR provides several important provisions highlighting user's control over their personal identifiable data, and consumer right to know and influence how their data is collected, stored and used.

The GDPR provisions related to individuals' data control, should be especially well considered in the context of the EHR. To ensure consumer's privacy and trust in EHR consumers should have a right to decide on how and with whom to share their data, they should also be able to access their record anywhere and anytime. Access to own health data encourages patients' ownership of their own care, makes them feel empowered as partners in their treatment.[9] Moreover, consumers should also have the possibility to delegate the management of these data to other persons such as a relative, a doctor and/or a pharmacist. A precise definition of 'management' should be provided beforehand, as well as rules on how that endowment of management responsibilities should take place.

Given the sensitive nature of health data, consumers should have a certain level of control of access to their information even by physicians, which can be done on the 'need-to-know' basis. For example, limits could be based on the role of the health care provider (e.g. a physical therapist or podiatrist should have less access than a primary care physician); date of the prior encounters (e.g. only health information within a certain number of years of the current visit would be available); type of health care provided (e.g. psychiatric records would not be available without separate permission of the patient); diagnosis (e.g. disclosure would be limited to information relating to a specific condition); or procedure (e.g. disclosure would be limited to information related to a specific procedure, such as a laboratory test, imaging study, or medication).[10] Patient summary[11] and or other

7 Forbrukerrådet, Health data for sale, 2017 https://fil.forbrukerradet.no/wp-content/uploads/2017/09/2017-09-06-report-privacy-eng.pdf

8 The Portuguese Association for Consumer Protection (DECO).

9 Gerard M, Fossa A, Folcarelli PH, Walker J, Bell SK What Patients Value About Reading Visit Notes: A Qualitative Inquiry of Patient Experiences With Their Health InformationJ Med Internet Res 2017;19(7):e237, DOI: 10.2196/jmir.7212

10 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3032388/

11 A minimum set of information o person's health needed to assure healthcare coordination and the continuity of care.

information relevant in case of emergency could be contained in a separate module more widely accessible in case of need (e.g. when the patient is unconscious).

The unnecessary disclosure of sensitive health information is more than a matter of privacy: it is a matter of public health. If access to personal health data is unrestricted, individuals with sexually transmitted diseases, mental illness, substance abuse, or other stigmatising conditions may simply avoid seeking medical help because of fear that that information about their condition will be widely accessible. Access restrictions are beneficial not only to the patients, but it also prevents healthcare professionals from scrutinising too much unnecessary information, for instance, a dentist filling a cavity does not need to have access to his patients' genetic test results.

Another crucial aspect of consumer control over their medical data is allowing the user to correct possible errors in their medical records or e-prescriptions. According to BEUC'S Danish member, Forbrugerrådet Tænk, the inability to correct and report on the errors in medical records and e-prescriptions in Denmark often results in undesired consequences for Danish consumers, including inaccurate disease history and incorrect medicine prescription. It is essential in order to ensure accuracy of the data and to avoid dramatic consequences for a patient. In EHR, for example, there could be an option for a user to insert a limited amount of characters available and without directly amending the electronic health record or deleting parts, in order not to raise liability issues. Health care professionals should take into account consumers' annotations and if relevant modify the content of the health records accordingly and in a timely manner. Moreover, consumers should be informed when the update has taken place.[12] The right to correct the data is also supported by the GDPR provisions on rectification.[13] **Therefore, while implementing EHR records across the EU, it is important to ensure that health and medical data of consumers is accurate and up-to-date; and mechanisms to correct medical errors must be enabled.**

1.2. Carrying out scientific health research in a responsible way

A balance between the interests of scientific health research and consumers' protection should be achieved through an adequate use of the GDPR provisions regarding exceptions and special provisions regarding scientific research.

Technical advances in health research have had broad implications in healthcare. Unprecedented amounts of health data and artificial intelligence tools permit processing of data previously considered impossible to study due to its volume and complexity. These new possibilities are likely to lead to scientific breakthroughs and significantly advance our knowledge on disease prevention and treatment. While considering the benefits of health data to scientific research, it is important to keep in mind that it is not only a source of valuable information but also very sensitive personal information.

[12] BEUC Position Paper, Electronic Health Record, 2011 http://www.beuc.eu/publications/2011-00399-01-e.pdf
[13] General Data Protection Regulation (GDPR) Article 16, 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Health data is considered a sensitive category of data under the GDPR and thus merits specific protection. The legal basis for processing sensitive categories of data are regulated in Article 9 of the GDPR. Consumer consent is a cornerstone of the legal regime that protects consumers' personal health data and it is safe to say that in principle personal health data should not be used without consumers' explicit consent. However, in reality there are other legal basis and exceptions for processing health data in addition to explicit consent. This affects how consumers' personal health data will be protected.

For instance, the GDPR allows the processing of health data for reasons of substantial public interest (e.g. serious cross-border threat to health), as well as for archiving purposes in the public interest, statistical, scientific or historical research purposes.

Moreover, scientific research is generally considered to be a compatible purpose for processing under Article 6(4) of the GDPR, so if the data has been initially collected under a lawful basis, there is further processing for a secondary research purpose is possible. This means that in the interest of scientific research, personal health data can be processed without getting consumers' explicit consent. What's more, as provided in Article 89 of the GDPR, Member States have some flexibility to modify consumers' rights (such as the right to access and rectify the personal data collected, or to object to the processing of their health data) when it is done for public interest goals, including scientific.[14]

Also, in those situations the health data is processed with the explicit consent of the consumer, it is important to note that recital 33 of the GDPR states that as it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research.

This exemption allowing personal sensitive data processing is aimed to facilitate scientific research and encourage new medical discoveries, however, depending on the rules of the Member States, there is a risk that the consumer could be left with little to no control over the use of their health data (especially genetic data). Countries are required to provide suitable data protection safeguards, but these safeguards may vary from one Member State to another because the GDPR leaves a certain degree of flexibility to Member States on this matter.

Overall, to maintain the balance between the needs of the scientific research community and patients' data protection, it is essential to ensure that consent derogations for scientific research are used legitimately and only when necessary.

Even though the GDPR allows consent derogations[15], it also implies the requirement of those collecting data to safeguard personal data. Safeguards include technical and organisational barriers to access, like an encryption, authentication requirements and user licences, or applying anonymisation[16] or pseudonymisation[17] that would 'no longer permit the identification of data subjects'.

---

[14] G Pormeister, Kärtm Genetic data and the research exemption: is the GDPR going too far? International Data Privacy Law, 2017,7 (2), 137−146.10.1093/idpl/ipx006.

[15] General Data Protection Regulation (GDPR) Article 9, Article 89, 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[16] Anonymisation refers to a technical process with the aim of irreversibly preventing the identification of individuals. Anonymised data do not fall under the scope of the GDPR.

[17] Pseudonymisation - the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is

Whereas anonymised data is no longer considered as personal data, in certain cases it may prevent researchers to fully benefit from the consumer's data for scientific research, as it may avert access to some important personal data categories. Therefore, when it comes to the use of personal data for health research purposes, it must be ensured that:

- The requirements laid down in the GDPR are fully respected;
- particular attention must be given to ensure the security and the quality of the data used in health research, and the respect of the principle of purpose limitation;
- The use of anonymised health data should be favoured, unless it would significantly impair the undertaken research. If anonymisation is not possible, data should be pseudonymised, so it can no longer be directly attributed to a specific person without the use of additional information. In this context, pseudonymisation is an essential safeguard and privacy enhancing technique which should be applied as a principle. However, it must not be forgotten that pseudonymous data is still considered personal data and therefore the requirements of the GDPR shall still be respected.

1.3. Artificial intelligence in healthcare

Artificial intelligence in healthcare must be applied in full respect of EU data protection rules, considering the principles of fairness, transparency, purpose limitation, data minimisation, accountability and privacy by design. Automated processes based on algorithms must be transparent to consumers and discrimination avoided.

The results of healthcare digitalisation will not be limited only to greater use of mobile health apps or implementation of the European electronic health record systems, its effects are reaching further than that. Digital health products and services produce enormous amount about health data of its users, which can be used to extract previously unknown information about human health and diseases. The analysis of such large data sets is called data mining and it serves as a foundation for artificial intelligence[18] (AI) and machine learning.[19]

AI and machine learning can truly transform the way diseases are prevented, treated and diagnosed. For example, when X-ray pictures are examined with the human eyes, detection of a small cancer tumour is not always possible and is often overlooked. Only if doctor suspects cancer during X-ray analysis, a more detailed examination using computer tomography (CT) scan is performed. The CT system displays a patient's body in a series of cross-sections. The larger the number of these cross-sections, the higher is the chance to detect an early-stage cancer. However, this means that the doctor must look at a larger number of images to detect a disease, and even after hours of image analysis a healthcare professional might not be as precise as 'mechanical eyes' of the specialised software could be.

kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable individual.

[18] Artificial intelligence – refers to systems that show intelligent behaviour: by analysing their environment they can perform various tasks with some degree of autonomy to achieve specific goals (e.g. in healthcare AI can be used to make faster and more accurate diagnosis).

[19] Machine learning – often confused with AI but machine learning takes the process one step further by offering the data necessary for a machine to learn and adapt when exposed to new data (e.g. in healthcare machine learning can be used to develop a very precise personalised treatment).

AI and machine learning can also pave the way to a more personalised treatment by analysing large amounts of information available on the condition/treatment and targeting it to a patient's needs. AI can also greatly contribute to what we know about the diseases and their prevention though processing large data sets from the electronic health records, genome sequencing, scientific databases etc. For instance, a Danish project on the use of machine learning is used to predict how many older people will need home nursing.[20]

There are also a number of risks that come along. The use of AI requires a large amounts of health data, which bears the risk of reduced consumer privacy, and not only when it comes to their medical history. For instance, AI can tremendously reduce the time doctors spend on filling in electronic health records by recording a patient-doctor conversation and transforming it into a written form.[21] However, our conversations with doctors are not always limited to the dry facts about the symptoms of the disease or details of treatment, although the technology will not distinguish this, meaning that our private conversations might be recorded. **Given high sensitivity of the health data, it is of key importance that AI is developed and used in full respect of EU data protection rules, considering the principles of fairness, transparency, purpose limitation, data minimisation, accountability and privacy by design.[22]**

There are numerous risks associated with AI when it comes to health applications or the use of AI in consumer markets in general. The more consumers interact with smart technologies, the higher the risk that situations of information and power asymmetries may occur, which impede consumers from taking informed decisions. In such an environment, consumers are highly vulnerable to be nudged by businesses into a specific choice of purchase. One may think of consumer behaviour when it comes to health-related decisions, for example such as nutrition or physical activity. AI in health services may also contribute to more inequalities when it comes to health of the population. For example, by analysing the socio-economic status and lifestyle of a consumer, combined with the data from their electronic health record, genetic data or family disease history, the algorithm will have a lot of information about the user's state of health and can make predictions/decisions which might negatively impact a consumer's ability to receive health insurance, treatment or service. Discrimination may also occur because of algorithmic-biases or the use of sensitive medical records in general. Thus, consumers may be deprived access to essential services.

From this follows that suppliers should develop AI in full compliance with legal standards. Users should have a right to transparency **so that they understand the characteristics of products including the logic of the algorithm functions. Discrimination should be avoided, and algorithmic control, for example by public authorities, must be ensured.**

[20] Danish Consumer Council Forbrugerrådet Tænk.

[21] Stanford Medicine, 'White Paper: The Future of Electronic Health Records', September 2018, http://med.stanford.edu/content/dam/sm/ehr/documents/SM-EHR-White-Papers_v12.pdf.

[22] BEUC position paper, 'Automated decision-making and artificial intelligence – A consumer Perspective', May 2018 https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf

2. Health data security - Clearing out regulatory insufficiencies

Consumers must benefit from digital health tools which respect privacy and security by design and by default principles.

Consumers' rights cannot be ensured unless their personal data is strongly protected by technology. If personal data can be accessed without prior authorisation or stolen, privacy is not guaranteed. Furthermore, lack of security of digital health devices can be a problem for the safety of its users: if a pacemaker is hacked, it is the user's own life that is at risk. Such risk is not hypothetical – it is very rea. For example, studies conducted in Belgium[23] and Norway[24] proved that many of connected health devices can be hacked which raise a lot of concerns over the security of personal data.

Therefore, it is essential to ensure security of health data both in case of system failure (e.g. virus causes loss of data) or an outside force caused damages (e.g. hacker attack). Even though it cannot be fully avoided, implementation of security by design and security by default principles could significantly minimise the risks.

Security by design means that all connected digital health products and services should incorporate state of the art cybersecurity functionalities at an early stage of their design process and before the products are put on the market.

Security by default means that the settings of a connected device and service are configured to the most secure setting by default. To ensure a high-level of security by design and by default, a minimum set of requirements for security should be binding for all connected products as a condition for putting them on the market.[25]

When it comes to digital health which comprises a wide range of different tools, the regulatory enforcement of 'security by design and by default' varies greatly depending on the type of the tool. For example, when the product is a wearable and connected device (e.g. fitness tracker), it is considered as a normal consumer good. Conversely, some of the products will fall under the category of medical device (e.g. pacemaker, neuro stimulator). With digital health being still a novel area, the regulation of its standards is fragmented across the EU.

2.1. Digital health as a critical infrastructure

Security of the digital medical systems in healthcare settings must be strengthened through the timely and diligent transposition and implementation of the NIS Directive.

[23] KU Leuven, Hacking Implantable Medical Devices to Emphasise Life-Threatening Security Flaws, 2017 https://www.esat.kuleuven.be/cosic/case-study-hacking-implantable-medical-devices-emphasise-life-threatening-security-flaws/

[24] Forbrukerrådet, Health data for sale, 2017 https://fil.forbrukerradet.no/wp-content/uploads/2017/09/2017-09-06-report-privacy-eng.pdf

[25] BEUC-ANEC Position Paper, Cybersecurity for Connected Products, 2018 http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

As healthcare is increasingly digitised and interconnected, medical systems are exposed to cybersecurity threats that can endanger a patient's health and safety. The EU recognises digital healthcare systems as a critical infrastructure. The ransomware attack WannaCry of 2017 which crippled hospitals in the UK has reconfirmed the need for strong IT security when it comes to digital health solutions. The EU's Directive on security of network and information systems (the NIS Directive) adopted in 2016 calls on the Member States to establish a national strategy for the security of network and information systems setting out strategic objectives and appropriate policy and regulatory measures. It also obliges the Member States to improve the cybersecurity of critical sectors operators, including health.

While the NIS Directive is expected to strengthen cybersecurity across the EU, not all EU Member States have met the deadline of May 2018 to transpose the Directive in to national law.[26] BEUC insists that all Member States must urgently meet the NIS Directive requirements, as strengthening of cybersecurity in medical systems cannot be further delayed.

2.2. Digital health as a medical device

In the context of the Medical Devices Regulation's provisions on IT security, the EU should ensure that it is implemented in full respect of the principle of security by design and by default. Further details should be provided on what is considered a minimum standard and how manufacturers should ensure it.

Digital health software intended for diagnostic, therapeutic or monitoring of physiological processes will fall under the definition of medical device or of an in-vitro diagnostic medical device and therefore may have to comply with the safety and performance requirements of the European Medical Devices Regulation (MDR) or In Vitro Diagnostic Devices Regulation (IVDR). This means that any tool meeting the definition as a medical device must comply with the safety and performance requirements set by the Regulation, and it will also be subject to post-market surveillance. In addition, consumers are entitled to contact a legitimate and competent partner in case of problems caused by using the tool.

Both MDR and IVDR are expected to strengthen consumers safety when using digital health solutions intended for medical purpose. For devices that incorporate software or for software that are devices in themselves, MDR require that the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation. MDR provisions also oblige the manufacturers to set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

Once applicable,[27] MDR and IVDR are expected to significantly strengthen consumer protection and security of their data while using digital health solutions qualified as a medical device. However, there is a need to provide further detail on what is considered a minimum IT security standard and how manufactures should ensure it. BEUC therefore calls on the EU to ensure that the provision on minimum requirements are implemented in full respect of the principles of security by design and by default.

[26] European Commissions, State-of-Play of transposition of NIS Directive, July 2018 https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

[27] MDR Its application date is set at 26 May 2020, following a three-year transitional period from its entry into force on 25 May 2017.

2.3. Digital health as a consumer product

A minimum set of security measures must be obligatory for all digital health connected products, including health and well-being apps as a condition for putting them on the market.

If a digital health solution is designed for a general purpose, it does not fall within the scope the MDR or IVDR scope, and this means that for the manufacturers of such solutions there is no obligation to meet minimum IT security requirements. Even though the EU is currently discussing provisions of the European ICT Security Certificate framework,[28] the capacity of this framework to protect consumers risks is limited if the proposal of manufacturers' voluntary participation in the framework is confirmed. The EU should not miss out an opportunity to strengthen IT security for the connected products, including for digital health.

2.3.1. Lifestyle and well-being connected products

The Radio Equipment Directive and the General Product Safety Directive must be updated to cover safety issues of digital health connected products falling outside of the scope of the Medical Devices Regulation.

Digital health as a consumer good and/or information society service is the subject of several other EU legislations, including the General Product Safety Directive[29] and Radio Equipment Directive.[30] However, provisions of the mentioned legislative files do not provide sufficient regulatory requirements on the IT security of such tools.

The concept of 'safety' is too narrow and fails to protect consumers from the security flaws which come along with connected devices such as lifestyle and well-being connected products thereby jeopardising the safety of the users.

This is because product safety is understood in the traditional sense only with regard to their potential harm to consumers' health and physical integrity such as through exposure to harmful chemicals and physical injuries. This concept of product safety is outdated knowing that devices which can connect to the internet can be hacked and thereby create new risks from a distance.[31]

Such a restrictive approach contributes to legal uncertainty, and there is a need to broaden the current safety regulatory framework to also include security. Because only then national market surveillance authorities would be obliged to take specific corrective measures to bring the product back to conformity whenever a product does not comply with the IT security requirements.[32]

The Radio Equipment Directive has the potential to address some of the security problems encountered in consumer connected products, including connected well-being devices falling outside of the scope of the Medical Devices regulation.

---

[28] Proposal for a Cybersecurity Act., http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf

[29] Directive 2001/95/EC on general product safety, 2001, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0095

[30] Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053

[31] BEUC-ANEC Position Paper, Cybersecurity for Connected Products, 2018 http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

[32] Ibid

Firstly, it applies to a significant number of consumer connected products, including connected well-being devices. Secondly, it contains relevant cybersecurity provisions such as a provision addressing the protection of personal data and privacy of the users of a Radio Equipment. Thirdly, it has the proper market surveillance mechanisms in place to withdraw these products from the markets.

However, while this Directive contains relevant security requirements, these are not fully operational yet. Some of the RED provisions, including the relevant cybersecurity ones, need a complementary secondary legislation (a delegated act) to be fully applicable and effective.

The General Product Safety Directive should also update the concept of 'safety' as currently it is too narrow and fails to protect consumers from the security flaws which come along with the connected devices.

2.3.2. Lifestyle and well-being apps

The EU should develop a comprehensive regulatory framework to ensure a harmonised approach and high privacy and security standards of lifestyle and well-being apps.

A big part of digital health solutions falling out of the medical device definition are mobile health applications defined as lifestyle and well-being apps.[33] The European Commission has acknowledged that this category is insufficiently regulated and has therefore attempted to bring more clarity on how to approach m-health apps. None of these attempts have however been successful.

Back in 2014, the European Commission set up a working group to develop guidelines for assessing the validity and reliability of the data that health and well-being apps collect and process. However, the group members failed to reach consensus on a set of guidelines, and the document was never developed.

In 2016, the European Commission facilitated drafting of the Code of Conduct by the stakeholder group on m-health apps[34]. The code was aimed to raise awareness of the data protection rules in relation to m-health apps, facilitate and increase compliance at the EU level for app developers. The draft Code covered several very important issues including privacy by design and by default, user consent and personal data breach. However, the draft Code of Conduct was not approved by the Article 29 Data Protection Working Party, and the current status of the Code of Conduct is unclear.

While a Code of Conduct could provide some essential guidelines to the manufacturers of lifestyle and well-being apps, BEUC insists that a comprehensive regulatory framework is needed. As a voluntary measure, a Code of Conduct is insufficient to ensure the safety of lifestyle and well-being apps. Such apps might contain a lot of sensitive health data and can have more impact on users' health than other apps by providing nutritional, sports or well-being advice. Harmonised privacy, security and safety standards are therefore required to safeguard consumers' health. The Commission should nonetheless closely monitor the work on the Code of Conduct which might serve as a complementary tool to ensure consumers' privacy and security interests in lifestyle and well-being apps.

---

[33] European Commission, Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps, 2014 https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and

[34] European Commission, Code of Conduct of mhealth apps, https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

The problem of regulatory ambiguity on lifestyle and well-being apps is also not sufficiently addressed at the national level although some countries are taking steps to provide a consumer with more information on mobile health applications, including those considered medical devices and lifestyle and well-being apps. According to Test-Achat, the Belgian government in collaboration with MedTech associations in 2018 launched an online platform 'mhealthBelgium' aimed to encourage companies to register their mobile health applications. The main idea is to ensure that both healthcare providers and patients have access to information on whether a mobile healthcare application meets the applicable rules and regulations, or regarding interoperability issues and, when applicable, be eligible for financial support in Belgium.

3. Safety of digital health solutions – additional measures needed

Digital health services and products must be safe and reliable to use.

With the variety of digital health products and services on the market, it is of key importance to ensure that they are safe and reliable for the consumer and do not pose risks to consumer health.

3.1. Safety of digital health products

As previously mentioned, digital health covers a great variety of products. The regulatory requirements for various products will depend on the nature of such products (e.g. whether it is a medical device, a connected product or an app). Considering that a higher risk of physical harm may occur because of the use of a digital medical device, BEUC particularly welcomes provisions of the Medical Devices Regulation (MDR). MDR includes several significant measures to protect consumer safety, including but not limited to stricter pre-market control, stronger rules on clinical evaluation and clinical investigation, stricter requirements on the use of hazardous substances and European Databank on Medical Devices (EUDAMED). Furthermore, the new Regulation also foresees a robust financial mechanism to ensure consumers are compensated in case they are exposed to defective products.[35]

Physical safety of other digital health products may fall under the scope of the General Product Safety Directive or Radio Equipment Directive. However as previously discussed, in the specific context of health products it is not sufficient to consider only physical safety, but the definition of safety must also include other aspects specifically related to security.

Market surveillance is another crucial aspect linked to the safety of digital health products. For instance, the MDR foresees closer coordination between competent authorities through information exchange and coordinated assessments, particularly in the area of market surveillance of devices.[36] As a follow up to the provision, the Joint Action on Market Surveillance of Medical Devices (JAMS) commenced in 2016 in order to improve the coordination between competent authorities and to develop a better common understanding of market surveillance for medical devices.[37]

[35] Regulation (EU) 2017/745, Medical Devices Regulation, 2017: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745
[36] Regulation (EU) 2017/745 ,Recital 84
[37] CAMD, Market Surveillance of medical devices, 2018: https://www.camd-europe.eu/wp-content/uploads/2018/05/JAMS_Information-for-manufacturers.pdf

However, JAMS can only be considered as a first step towards a European-wide coordination of market surveillance, but it is not a pan-European market surveillance system itself. Therefore, there is still a need to strengthen the surveillance and reporting mechanism across the EU. Furthermore, an increased number of controls should not be limited to a particular group of products, as an adequate market surveillance system is needed for all products, including all digital health products falling outside of the scope of the MDR.

In the context of other consumer products (including digital solutions), the lack of market surveillance has been pointed out by many players in Europe, including consumer organisations, the industry, the European Parliament, and the European Commission.[38] Member States do not sufficiently cooperate at the EU level and among each other which makes it difficult to take unsafe products off the shelves. Insufficient level of safety and lack of cooperation are partly explained by the fact that the Member States do not invest adequate resources in market surveillance. Consequently, there is not enough staff who can sample products, and there are not enough financial and technical resources available for testing in laboratories. While testing for medical devices is covered by the MDR, the biggest group of digital health products remains insufficiently tested across the EU, which leads to a compromised safety of such tools. **BEUC calls on the European Commission to ensure better market surveillance rules which are needed for all consumer products, not only harmonised ones. Joint testing and enforcement should also be carried out for various digital health products not covered by the MDR.[39]**

3.2. Safety of digital health services

Digital health includes not only a variety of products but also many services ranging from an online consultation to a medical intervention. How different are digital health services from traditional health care services? Digital health services should not differ from traditional 'offline' services, and it should be performed only by qualified professional, while a medical advice/action facilitated by a digital medical device must be based on scientific evidence and designed in a way minimising health risks to consumers. Furthermore, in some cases digital health solutions such as teleconsultation or apps might serve as a safer and more comprehensive alternative than Dr. Google which is often used to make DYI medical diagnosis by many internet users.

Having said that, the reality is that the approach to such services greatly varies across EU Member States. EU law applies to telehealth as a healthcare service only when it comes to cross-border health. Other than that, requirements for such services uniquely belong to the national level. At the EU level, when a telehealth service is delivered beyond national borders, the EU Cross-Border Healthcare Directive is set to protect patient rights. These rights include but are not limited to the right to receive the medical treatment in another country, right to be informed on the quality and safety of the service used or the right to complain. However, the Directive seems to apply to certain aspects applicable to telehealth while it might not be applicable to others.[40] This ambiguity could potentially compromise the safety of digital health services and lead to the situations where it is unclear which liability mechanisms a consumer can use in cases where a service caused damage.

---

38 EC Impact Assessment on the Regulation on enforcement and compliance.

39 BEUC, ANEC (2018) Ensuring consumers' safety – What way forward for Market Surveillance in the EU? https://www.beuc.eu/publications/beuc-x-2018-030_ensuring_consumers_safety_-_what_way_forward_for_market_surveillance_in_the_eu.pdf

40 Raposo VL. Telemedicine: The legal framework (or the lack of it) in Europe. GMS Health Technology Assessment. 2016;12:Doc03. doi:10.3205/hta000126.

For instance, when telehealth is delivered as a healthcare service, some open issues remain as regards the requirements for health professional's qualification and registration in order to practice telemedicine. These aspects are crucial for telehealth service liability, as they are directly linked with the questions of legal consequences of a treatment provided through telemedicine. First of all, health professionals are not legally required to have an extra qualification to practice telemedicine, which in some cases is fully understandable. But when it comes to such services as teleintervention an absence of specific qualification normally not required in conventional medicine might lead to severe implications for patient's health.

In addition, according to EU legislation, a healthcare professional offering telemedicine needs only to be registered in the country where he/she is physically established. Yet it is not clear whether a physician must be registered first for traditional healthcare practice to be then allowed to practice telemedicine.[41] The EU Directive on the recognition of professional qualifications does not apply to healthcare professionals providing cross-border telemedicine, as it only covers healthcare professionals that physically move to another Member State to practice their profession. This is an important aspect to take into account, as what is considered 'regulated' health professionals differ across the EU Member States. For example, there are different approaches to 'traditional' and 'complementary' health professionals (e.g. homeopaths, naturopaths) and in some countries such professions are regulated, in some not.[42]

Furthermore, when it comes to telehealth as healthcare service (or a medical act), the big question is what is considered to be a medical act. Some national legal systems, such as Poland, require the physical presence of the patient and health professional at the same time and in the same place, for a medical act to be legally valid.[43]

The described above situations are largely regulated at the national level. But despite these different approaches to healthcare services it is of key importance to increase the safety of telehealth services through the harmonisation of certain rules, for instance as regards healthcare professional's qualification in telemedicine, definition of what constitutes a medical act as well as establishing a common approach on liability of the cross-border telehealth services across the EU. Furthermore, depending on the nature of a service, not all digital health services might be medical services regulated either at the national level or by the European Cross-Border Healthcare Directive. Some services (e.g. teleconsultation with a nutritionist) might fall in the category of general services, and currently there is no European legislation regulating this category. The necessary steps should be taken to close this gap for an enhance consumer safety.

[41] Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine'.

[42] Wiesener, S., Salamonsen, A., & Fønnebø, V. (2018). Which risk understandings can be derived from the current disharmonized regulation of complementary and alternative medicine in Europe? BMC Complementary and Alternative Medicine, 18(1). doi:10.1186/s12906-017-2073-9.

[43] EU legal framework to telemedicine services, SWD(2012) 414 final.

4. Additional measures to protect consumers

Legislative measures such as strong market surveillance, law enforcement, as well as efficient redress tools on digital health products and services must be put in place to contribute to an effective protection of EU consumers.

In addition to addressing some existing regulatory gaps, it is also important to take additional measures such as carrying out market surveillance and introducing redress to ensure safety and security of the European consumers.

4.1. Redress mechanisms to enhance consumer protection

Many digital health devices and service solutions are used on a massive scale. However, consumer protection mechanisms are not always clear in case these devices and services cause damage. Legal proceedings are expensive, time-consuming and the compensation amounts might not always be large. For small amounts, it is usually not economically viable for people to go through legal proceedings on their own, but the frustration remains.

Collective redress mechanism provides a number of consumers with an opportunity to jointly bring a court case to obtain compensation for damage which arises from the same source. Currently only five of the EU countries enjoy efficient collective redress system (Belgium, Italy, Portugal, Spain and Sweden), in other countries the collective redress system either does not exist or contains serious flaws or has been introduced to recently to be evaluated.

In 2018, the European Commission announced a proposal for a directive on representative actions for the protection of the collective interest of consumers. The Commission's proposal also foresees availability of individual remedies for consumers harmed by unfair commercial practices (e.g. a misleading marketing). Under the proposals, consumers would be afforded both contractual and non-contractual remedies, including the right to terminate an infringing contract and compensation.

BEUC strongly welcomes the Commission's proposal on representative actions. It is crucial to give consumers a realistic chance to obtain redressing case of mass damages, as in case of infamous PIP breast implants scandal.[44] **Given the specific nature and higher risk level of digital health devices and services it is crucial to include such devices and services within the scope of the above mentioned draft law**.[45]

4.2. Enforcement of the existing legislation

Following the technological advancement, the EU has already made some significant steps in adjusting regulatory frameworks to a new reality. The GDPR, MDR, NIS Directive, Cross-Border Healthcare Directive are critical for successful healthcare digitalisation across the EU. However, good laws need to be properly rolled out. Therefore, enforcement of the existing legislation affecting digital health is necessary to address the risks to consumer safety, privacy and security coming from possible non-compliance with the existing laws.

---

[44] BEUC response to EC ex-post consultation 'Proposal for a Directive on representative Action', 2018: https://www.beuc.eu/publications/beuc-x-2018-042_representative_action.pdf

[45] BEUC Position paper 'A new Deal for Consumers – Revision of the Injunctions Directive', January 2018: https://www.beuc.eu/publications/beuc-x-2018-004_a_new_deal_for_consumers.pdf

The lack of effective enforcement is a key problem in consumer protection. At the same time, it is a complex problem to tackle, as effective enforcement depends on multiple factors such as the enforcement structure and traditions at national level, strong public authorities, the economic climate, the strength and experience of consumer organisations and the possibility for easy redress. A major factor of difficulty is linked to the fact that there are grey zones as to which public authorities are competent, which then leads to lack of action.

We therefore call for more cooperation among various enforcement bodies and organisations as well as to strengthen the powers and sanctions available to them.

5. Digital health for all

Digital health solutions can provide consumers with numerous opportunities to improve health and well-being and to better manage diseases. However, can digital health provide this to *all* consumers or are its benefits accessible only to younger, highly educated, and digital literate users in more economically developed countries and regions?

5.1. Internet connection for all

Digital health solutions should be promoted only along with access to an affordable, high-quality, high-speed internet connection to enable safety and accessibility of such solutions for all.

Being connected to the internet is a crucial precondition of digital health, and digital health solutions cannot become a reality for all until every EU citizen has an affordable, high-quality and high-speed internet connection. Furthermore, a good internet connection is a prerequisite to user's safety as it is the only way to guarantee non-interrupted functioning of a product and provision of a service.

In the EU-28 there is still an urban-rural divide in terms of internet access. In 2017, 82% of rural households had access to internet compared to 90% in cities and 87% in towns and suburbs.[46] It all might seem as dry statistics until there is a realisation that behind these numbers there are people not being able to use a digitalised health service because they do not have an internet connection. In some EU countries (Greece, Portugal, Bulgaria, Romania) the digital divide between urban and rural is particularly strong, and further healthcare digitalisation without ensuring internet access for all can result in more inequalities. Thus, health digitalisation can only go hand in hand with the establishment of better internet connectivity for all Europeans.

The EU's commitment to ensure the availability and take up of very high capacity networks enabling the widespread use of products, services and application is expressed in the European Commission's strategy on Connectivity for a European Gigabit Society.[47]

[46] Eurostat, Digital economy and society statistics - households and individuals, 2017 http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

[47] European Commission Communication Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society, 2016 https://ec.europa.eu/digital-single-market/en/news/communication-connectivity-competitive-digital-single-market-towards-european-gigabit-society

5.2. All-inclusive digital health solutions

Consumers have different needs, capacities, values and goals when it comes to use of digital health. BEUC insists that digital health solutions must correspond to the variety of users' preferences, also respecting a preference not to use a digital health product or service. The levels of digital health literacy should also be improved both among consumers and healthcare professionals.

Several studies[48] have shown that individuals with limited (digital) health literacy skills not only consume less online information sources, but also gain less positive outcomes (e.g. less self-management of healthcare needs) from online sources. Research has also shown that most digital tools are not well designed for vulnerable populations, such as older adults and adults with limited health literacy skills. Moreover, most digital health solutions are developed with the intention to empower consumers and provide them with self-management tools, but it is crucial to remember that not all consumers are positioned or willing to self-manage their health.

To diminish the risk of a digital divide and increase the usefulness and uptake of digital health solutions, it is important to consider the following aspects throughout the development of such solutions[49]:

- Specific needs of the targeted group;
- Access to the tool;
- Literacy level;
- Language skills;
- Potential incapacities;
- Cultural sensitivities, habits and beliefs.

To make a digital health tool useful, accessible and addressing users' needs, it is of key importance to involve future users with diverse perspectives, circumstances, capacities and experiences when designing the tool. For example, in Denmark there are several initiatives aimed to address the specific needs of patients with multiple chronic conditions. One of such initiatives is a project called Epital Care Model (ECM). ECM was established in a Danish municipality which allowed for the freedom of redesigning health care processes. The pilot project focussed on patients with chronic obstructive pulmonary disease (COPD). It aimed at giving them better control of their condition while reducing their visits and admissions to the hospital and support continuity of care. The participants were provided with the tablet-based access to a 24/7 response and coordination center that coordinated both virtual and face-to-face support for COPD management. Depending on the well-being of the participants, some of them were offered two additional services: an outgoing acute medical team and a local subacute bed function.[50] The pilot project resulted in the improved COPD management and increased quality of life of the participants: the remote service allowed patients to travel and be more active, as the digital health solution was meeting all their needs and did not require frequent visits to the hospital.

---

[48] Bol, N., Helberger, N., & Weert, J. C. M.. Differences in mobile health app use: A source of new digital inequalities? The Information Society, 2018, 34(3), 183-193.https://pure.uva.nl/ws/files/25256057/Differences_in_mobile_health_app_use.pdf

[49] Latulippe K, Hamel C, Giroux D. Social Health Inequalities and eHealth: A Literature Review With Qualitative Synthesis of Theoretical and Empirical Studies. Eysenbach G, ed. Journal of Medical Internet Research. 2017;19(4): e136. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5427250/

[50] Phanareth K, Vingtoft S, Christensen AS, Nielsen JS, Svenstrup J, Berntsen GKR, Newman SP, Kayser LThe Epital Care Model: A New Person-Centered Model of Technology-Enabled Integrated Care for People With Long Term Conditions, JMIR Res Protoc 2017;6(1):e6, DOI: 10.2196/resprot.6506

Not all consumers necessarily want to use digital health service or product, therefore this preference should also be respected by having an alternative to digital health product or service, where possible. While considering different needs of diverse consumer groups, it is also crucial to improve the level of digital health literacy both in consumers and healthcare professionals in order to increase the uptake of digital health solutions, as well as their benefits to the users.

6. The many faces of digital health and why a streamlined approach is needed

Digital health products and services must complement and improve national healthcare systems and services provided to consumers.

A streamlined approach to digital health solutions implementation is also crucial for the national level. With the growing number of various digital health opportunities, many countries are introducing such digital health products and services into healthcare systems. However, lack of an integrated and streamlined approach may cause an undesirable effect of being burdensome for its users and providers.

The Portuguese Consumer organisation DECO provides an example of a digital vaccine bulletin implemented in Portugal. A paper version of the vaccine bulletin no longer exists, and this causes access problems for elderly and people what do not have access to internet or have low digital literacy. Moreover, vaccination performed in private healthcare settings is not registered in the bulletin.

In addition to poor execution of potentially good ideas, many countries are facing the consequences of low awareness on different aspects of health digitalisation. According to the Belgian Consumer organisation Test Achat/Test Aankoop, despite digital health solutions being introduced into the Belgian healthcare system, there is a lack of information for consumers on how they can benefit from such tools. The problems with informed consent are also often reported, as there is insufficient understanding of when consent can be considered informed. Furthermore, Belgium has recently faced a situation of health data of thousands of citizens being publicly available due to a mistake done by a company scanning the medical record archives to transform them into the digital form. It also appeared to be that in addition to a failure to securely present scanned data to the hospitals, the scanning company won an initial tender by ensuring low price through having scans carried out in social settings and prisons.[51] With GDPR coming into force, the digitalisation of patient files can only be carried out by certified companies with employees who have been screened I advance.

The Norwegian Consumer Council Forbrukerrådet also reports the lack of involvement of the Norwegian general practitioners (GP) into the electronic health record system, which is currently based on the voluntary participation of the doctors. Even with EHR system in place, not all Norwegian consumers may benefit from it, as it would depend on the GP willingness to use it, as currently the novel system is more burdensome than traditional one.

[51] Skipr 'Medische gegevens op straat door datalek', 2016 https://www.skipr.nl/actueel/id25258-medische-gegevens-op-straat-door-datalek.html

For a consumer to truly benefit from digital health products and services, they should be well-integrated into the existing systems, such solutions should not be burdensome nor to their users, neither to their system itself.

Concluding remarks

Newly emerging technology is changing the way that health and care is provided. Electronic health record, health apps, big data, artificial intelligence and machine learning are just around the corner ready to enter the European healthcare systems and transform the traditional way of preventing, diagnosing, treating diseases and caring for our health. The healthcare's future is digital, however are we ready for such a future? It seems not yet, as there are still regulatory insufficiencies to address to enhance the benefits of digital health products and services for consumers. Even though filling in regulatory gaps is crucial, it is not less important to base policy decisions, research advancement and device development on the interests and needs of the end user – consumers, as it is the only way to ensure an optimistic scenario of the digital health future.

ENDS

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).