Digital health and wellbeing: the case for broadening the EU DigComp framework

Anícia Rebelo Trindade [1], Debbie Holley [2], Célio Gonçalo Marques[3]

[1] Polytechnic Institute of Tomar, Portugal
Educational Technology Laboratory (LabTE)
University of Coimbra, Portugal
Anicia.r.trindade@gmail.pt
[2] Department of Nursing Sciences
Bournemouth University, England
dholley@bournemouth.ac.uk
[3] Polytechnic Institute of Tomar,
Laboratory of Pedagogical
Innovation and Distance Learning (LIED.IPT)
Portugal
celiomarques@ipt.pt

Abstract. Digital health and wellbeing are highly contested terms and range from carefully costed and evaluated software systems designed for patients to access their doctor; mobile applications that are evidence based to support those living with long term health conditions such as diabetes; to the Coronavirus travel applications (app) developed to enable societies to come together post-pandemic. This is contrasted with numerous mental health 'apps' that are reported to be particularly problematic, with their tracking algorithms and individual personal data being sold on to third parties. Against this fast-changing backdrop, the European Union (EU) launched the revision of their Digital Framework Digital Competence (DigComp 2.2) in February of 2022. This paper reports on the findings of the 'Safety and Security' working group and their recommendations for the digital knowledge, skills, and attitudes (KSA) required for EU citizens negotiating a complex and constantly changing health sector.
Keywords: EU DigComp, Digital health, wellbeing, long term health

1 Introduction

The fast increase of Artificial Intelligence (AI) health systems and applications bring together the necessity of empowering all citizens of critical knowledge, skills, and attitudes (KSA) to make informed choices when interacting, using, and installing on their smart devices those applications. The advanced techniques related with machine learning, and deep learning, allows data analysis in order to facilitate new knowledge in different areas of Health Sciences (Chang, 2020); yet according to Murdoch (2021) many advances in healthcare artificial intelligence technologies end up owned and controlled by private entities, raising the huge discussion about protecting patient health information. Competencies such as: protecting devices, protecting personal data and privacy, and protecting health and well-being are essential to avoid threats none also for physical, emotional, and personal health, as well as to avoid poor protection of

patient data privacy (Murdoch, 2021). Regarding the AI health concerns, the framework also brings the relevance for a comprehensive understanding about what AI systems do and what do they not do; how do AI systems work; how to interact with AI systems for different daily routines (look for information, using AI systems and apps; focusing on privacy and personal data), and the challenges and ethics of AI, and the attitudes regarding human agency control (Vuorikari, Kluzer & Punie, 2022).

Following the update of the DigComp Framework, a group of experts in the areas of safety, security, and wellbeing, contributed to the articulation of the appropriate KSA in the scope of digital safety security and wellbeing, to promote a confident, critical, and responsible use of digital technology, where the use of AI health systems and apps take place. The study submitted a series of recommendations about the KSA, and were framed by the research question:

RQ: Do European Union (EU) citizens need to engage with the digital environment in a confident, critical, and responsible way for participation in society in the safety area of the DigComp framework?

To answer this challenge, qualitative research was conducted and designed by a group of experts, working as part of the wider Community of Practice (CoP), using a Design-Based Research (DBR) approach (Mckenney & Reeves, 2014; Plomp, 2013), to propose the new KSA encompassed in the revised European DigComp 2.2 framework for safety, security, and well-being competencies, required for EU citizens negotiating a complex and constantly changing of health sector.

2 Background

2.1 Digital health and security

The General Data Protection Regulation (GDPR) framework is no longer adequate nor sufficient to cover the complex problems emerging from the capture and treatment of sensitive data (Fornasier, 2021). Empowering citizens to know how to protect their own personal data, is becoming a huge challenge, requiring new policy implementation approaches. Nowadays, the currency of many companies and organisations is the information/data they harvest from individuals, both about their personal data and their health and medical conditions. For Seh et al (2020), a data breach means the illegal disclosure or use of data information without authorization of the main information owner. As we outline, data breaches are not just a concern and complication for security experts but are now threatening the ordinary citizen (Seh et al, 2020). EU citizens need to embrace the digital to secure employment, to communicate, to shop, and increasingly to access health apps and systems regarding their own physical and mental health needs. As Goldsmith, Holley & Quinney, (2020) explain, "human learning, underpinned by technological tools, needs to be partnered by a focus on lifelong learning and continuous professional development."

Chang (2020), advocates for the outcomes of good predictions of human health conditions, and considers health data from an open access view, to be released and shared without any obstacles. In this way, AI will flourish and lead to discovering new knowledge from all sources of data and information, and then, help the healthcare

professionals make the best decisions. Fornasier (2021) anticipates it will become the new 'normal' to expect patients to engage with their digital health tools more than their more standard user profile.

However, there are more dystopian views about the use and value of data capture and analysis. Regarding protecting devices, it is important that all citizens, are able to "weigh the benefits and risks of using biometric identification techniques (e.g., fingerprint, face images) as they can affect safety in unintended ways. If biometric information is leaked or hacked, it becomes compromised and can lead to identity fraud" (Vuorikari, Kluzer & Punie, 2022, p. 36). Today, people's personal information is constantly at risk, (Singh et 2021 p1), who comment that, "Smart healthcare uses advanced technologies to transform the traditional medical system in an all-round way, making healthcare more efficient, more convenient, and more personalized. Unfortunately, medical data security is a serious issue in the smart healthcare systems". Providing guidance for the citizens to identify their sensitive data and know how to protect it from third parties (Center for Open Data Enterprise (CODE), 2019) is no longer a problem only for third party organizations.

Protecting privacy health data involves understanding what extended health applications and systems utilized codes that make it possible to link data about an individual without revealing the person's identity (CODE, 2019). In this regard, it's still important that citizens be "aware that for many digital health applications, there are no official licensing procedures as is the case in mainstream medicine" (Vuorikari, Kluzer & Punie, 2022, p. 38), and being able to assume the responsibility for protecting personal and collective health and safety when evaluating the effects of medical and medical-like products and services online, as the internet is awash with false and potentially dangerous information about health (Vuorikari, Kluzer & Punie, 2022, p. 38). As Singh et al (op.cit) explain, comprehensive state-of-art-techniques are required, and they look to solutions from notable cryptography, biometrics, watermarking, and blockchain-based security techniques for healthcare applications.

3 Methodology

3.1 European DigComp revision

A decade ago (Ferrari, 2012), the European Commission started the discussion about digital competence, and how to empower citizens to the digital era, to interact with digital technologies. The work done created the first European Digital Framework, DigComp (Ferrari, 2013), proposing five main areas that the EU thought need to be developed by any citizen. Among these areas, the safety area, include competences such as: 4.1 - Protecting devices; 4.2 - Protecting personal data and privacy; 4.3 - protecting health and well-being, and protecting the environment (Vuorikari, Kluzer & Punie, 2022).

The European Commission (2022) launched the newest version of the digital competence framework, including the KSA gathered by different expert groups in each field area of the framework. The research question that underpinned the one-year body of work leading to the launch was: what knowledge, skills and attitudes do citizens need to engage with the digital environment in a confident, critical, and responsible way for

learning, at work, and for participation in society in the safety area of the European DigComp 2.2 revision framework? The research was designed using a based-research (DBR) protocol, to combine the theory with practice, also representing the voices of all stakeholders (experts, volunteers, and JRC leadership).

The experts organized the DBR approach into four cycles, as proposed by Plomp (2013) involves: i) analyze existing practical problems; ii) develop innovative solutions based on existing design principles; iii) create iterative cycles of tests for the improvement of the solutions in practice; iv) reflect on the principles of improvement of the implemented solutions.

Following the DBR approach, the DigComp revision model was organized into eight phases. In the first phase the European Commission and the Joint Research Centre (JRC) set out the scope and scale of the challenge, and the different working groups addressed the emergent themes in the digital world, namely digital health, digital safety and security, AI applications, safety and security and well-being.

In this regard, the analysis of existing practical problems was conducted on phase one and two, where different tasks were undertaken: i) identification of the new digital competence requirements for citizens which stem in the digital world, based on literature review and brainstorming and focus group sessions; ii) Propose and select requirements for a safety, security and well-being, linked to the different competences of the Framework 2.1; iii) organization of three strands of discussion: E-Health/well-being; opportunities and limits to digital protection; how to build safety and security step by step in the development of users (cf. younger students, active workers, and elderly people).

For the development of innovative solutions based on existing design principles cycle took place on phase three and four: i) conducting a literature review about the themes that inform the scope of safety, security and well-being; ii) applying underpinning literature and values triangulated back through to the DigComp 2.1 framework; iii) initial suggestions for relevant knowledge, skills and attitudes (KSA), statements related to the requirements previously identified, along with suggestions about where they might fit into the safety area of DigComp framework 2.1 (digital competence 4.1 protecting devices; 4.2 protecting personal data and privacy; and 4.3 protecting health and well-being).

The cyclic creation of iterative sequences of tests for the improvement of the solutions in practices was accomplished in phase five and six, where: i) an iterative peer review/reflective cycle of work was undertaken, using online questionnaires, and organizing brainstorming meetings, and focus group discussions, involving more than 373 stakeholders/experts and more than 31 experts in the field of safety, security and well-being, across Europe, as well as the expertise, consultation and validation of experts, stakeholders and civil society). In these phases the group of experts collect more than hundred statements (n=133) for the safety area (51 statements (KSA) related with the digital competence “protecting devices” and its components; 41 statements (KSA) related with “protecting personal data and privacy”, and 41 statements related with “protecting health and well-being”). Considering the definition of KSA presented in the theoretical framework, a knowledge statement starts with: “knows/aware/understands that… or aware of”. The skill statement begins with “knows how/can apply…, etc.”. Finally, an attitude sentence starts with “inclined to/assumes responsibility/wary of/confident in… etc.). Closing the DBR protocol approach,

reflecting the principles of improvement of the implemented solutions developed by the JRC on phase seven and eight, came up with a proposed list of KSA, some of which were directly applied and incorporated into the DigComp 2.2 version.

For data collection, direct techniques and indirect documentation techniques were used (Tuckman, 2012). The direct data collection techniques integrate three questionnaire surveys (used and applied to validate the KSA for each of the three digital competence of safety areas (4.1 - protecting devices; 4.2 - protecting personal data and privacy; and 4.3- protecting health and well-being).

The first part of the surveys collect data related to the characterization of the respondent. The second part of the survey measures the clarity of the KSA statement and the level of relevance of the statement with a Likert scale with five points. Each survey includes only 20 statements chosen by the JRC, among all statements collected by the experts through phase three and four (see table 1). Before the online public validation through the surveys on phase five and six, on phase seven and eight only few were selected to be included on the Digcomp 2.2 update (see table 1). The survey also collected additional comments about the Digcomp 2.2 update, which were useful to rephrase some proposed statements. The survey was completed online by a broad range of stakeholders, from different countries and organizations across Europe. Despite a limited response useful information was collected.

Table 1. Process of selection of KSA for DigComp 2.2 update

Digital competence	no. KSA proposed by experts (phase 3 and 4)	no. KSA selected by JRC for survey validation (phase 5 and 6)	no. KSA selected by experts related with digital health and AI	no. of KSA selected through public validation to DigComp 2.2 (phase 7 and 8)
4.1 - Protecting devices	51	20	17	14
4.2 - Protecting personal data and privacy	41	20	16	9
4.3 - protecting health and well-being	41	21	12	14
Total	**133**	**61**	**45**	**37**

Source: Expert working group statements (KSA) results regarding digital competence 4.1, 4.2 and 4.3, survey validation results and final statements of DigComp 2.2 at Vuorikari, Kluzer & Punie, 2022, p. 35 – 40.

4 Results and Discussion

This section presents the results of the methodology procedure to collect the KSA statements on the safety area, presenting only those that the experts considered that relate to digital health safety security and wellbeing among the 20 statements per each competence submitted to public validation (see table 2).

4.1 Results protecting devices

The competence of protecting devices, covered previously invisible types of KSA such as identity theft, psychological manipulation, cyber-attacks, vulnerabilities, and protection against malicious software. The experts believe that those KSA (n= 5), that

were not covered by the DigComp framework, are still very important, regarding the threats and risks that all citizens face in their daily routine (see table 3). This is supported by the work of Seh et al, (2020) who clearly identify data breach as one of the major concerns of digital health data protection.

Table 2. Examples of final KSA related with digital health for digital competence 4.1 - protecting devices presented in the survey validation and were reframed or excluded of the DigComp framework 2.2

	Dimension 4		Decision		
Type	**Nr. Stat.**	**Statement**	**Included**	**Not Included**	**Included with Arrangements**
Knowledge	3	Aware of the risk of identity theft on the internet, someone commits fraud or other crimes using another person's personal data (digital identity, username) without their permission.			X
	4	Aware of "social engineering" that uses psychological manipulation to obtain confidential information (passwords, pin-codes) from victims or convince them to take a harmful action (execute malicious software).		X	
	5	Understands that IoT applications can be vulnerable to cyber-attacks as they require the exchange of data via wireless networks.		X	
	6	Knows that cybercriminals might have several motivations to conduct their unlawful activity (motivated by financial gain, protest, information gathering for spying).		X	
	8	Knows about the importance of keeping the operating system and applications (browser) up to date to fix security vulnerabilities and protect against malicious software (malware).	X		
	9	Knows that a firewall blocks certain kinds of network traffic aiming to prevent a number of different security risks (spam, denial of service, remote logins).	X		
Skills	1	Knows how to adopt a proper cyber-hygiene regarding passwords (selecting strong ones difficult to guess) and managing them securely (password manager).	X		
	2	Knows how to activate two-factor authentication for important services.	X		
	3	Acquires digital tools that do not process unnecessarily personal data, check the type of data and features an app access on one's mobile phone.			X
	4	Able to encrypt sensitive data stored on personal devices or in a cloud storage.	X		
	5	Can identify the affordances of different data hosting/storing services, file versioning features of cloud storage to revert to previous files in case of corruption or deletion, to compare file versions to one another).		X	
	6	Knows how to install and activate protection software and services (antivirus, anti-malware, firewall) to keep digital content and personal data safe.	X		
	7	Can respond to a security breach (an incident that results in unauthorized access to digital data, applications, networks or devices), a personal data breach (leakage of their login and passwords) or a malware attack (contain viruses) or a malware attack (ransomware).			X

	Dimension 4		Decision		
Type	**Nr. Stat.**	**Statement**	**Included**	**Not Included**	**Included with Arrangements**
Attitudes	1	Vigilant not to leave computers or mobile devices unattended, for example in public places (in a restaurant, train, car).			X
	2	Weighs the risks and benefits of using biometric identification techniques (fingerprint, face images) as they can affect safety in unintended ways (biometric information can be leaked or hacked and therefore become compromised).			X
	3	Vigilant towards practices to protect devices and digital content as security risks are always evolving.		X	
	4	Keen to consider some self-protective behaviours such as not using open wi-fi networks to make financial transactions or online banking.	X		

Source: Survey validation statements (KSA) results regarding protecting devices and final statements of DigComp 2.2 at Vuorikari, Kluzer & Punie, 2022, p. 36.

4.2 Results Protecting personal data and privacy

Regarding protecting personal data and privacy, the group of experts selected 16 of the 20 statements submitted to public validation, which were related to digital health behaviours that all citizens need to acquire, in order to protect them and others, against risks and cyber-attacks of data health information. Nevertheless, half of these KSA were not covered in DigComp 2.2 (n= 8).

Table 3. Examples of final KSA related with digital health for digital competence 4.2 - protecting personal data and privacy presented in the survey validation and were reframed or excluded from the DigComp framework 2.2.

	Dimension 4		Decision		
Type	**Nr. Stat.**	**Statement**	**Included**	**Not Included**	**Included with Arrangements**
Knowledge	1	Aware that secure electronic identification is a key feature to enable the safe sharing of personal data with third parties when conducting public sector and private transactions.	X		
	4	Aware that a security or privacy incident can result in loss of control, compromise, unauthorized disclosure, acquisition, or access to personal data, in physical or electronic form.		X	
	5	Knows that, in terms of the EU's GDPR, even voice interactions with a virtual assistant are personal data and can expose users to certain data protection, privacy and security risks.		X	
	6	Knows that processing of personal data encompasses the collection, recording, organisation, storage, and modifications of the data. When an AI system links different pieces of apparently anonymous information together, it can lead to de-anonymisation, the identification of a particular person.			X
	7	Recognise that voice assistants, chatbots, smart devices and other AI technologies that rely on users' biometric and other personal data might process such data more than is necessary (it is considered disproportionate and violates the principle of proportionality specified by GDPR).		X	

	Dimension 4		Decision		
Type	**Nr. Stat.**	**Statement**	**Included**	**Not Included**	**Included with Arrangements**
	8	Knows that reading a "privacy policy" of an app or service explains what personal data it collects and whether data is shared with third parties possibly including information about the device used (brand of the phone) and geolocation of the user.			X
	9	Knows how to identify suspicious email messages that try to obtain sensitive information (personal data, banking identification) or might contain malware.			X
Skills	1	Knows how to modify privacy settings to keep safe from unwanted contacts (spam texts, emails).	X		
	4	Uses digital certificates acquired from certifying authorities (digital certificates for authentication and digital signing stored on national identity cards).			X
	5	If informed by data controllers that there has been a data breach affecting users, act accordingly to take actions to mitigate the impact (change all passwords immediately, not just the one known to be compromised).		X	
	6	Can help mitigate the risks of personal data breaches by expressing concerns to relevant authorities relating to the usage of AI tools that collect data, especially if there is a suspicion that there is a violation of the GDPR or when the company does not make the information available.		X	
Attitudes	1	Emphasises the importance of taking a conscious decision whether to share information about private life publicly, considering the risks involved (especially for children) while keeping control of the personal data.		X	
	2	Weighs the benefits and risks before activating a virtual assistant (Siri, Alexa, Cortana, Google assistant) or smart IoT devices as they can expose personal daily routines.			X
	3	Weighs the benefits and risks before engaging with software that uses biometric data (voice, face images), checking that it complies with GDPR.		X	
	4	Weighs the benefits and risks before allowing third parties to process personal data, recognises that voice assistants that are connected to smart home devices can give access to the data to third parties (companies, governments, cybercriminals).		X	
	5	Confident in carrying out online transactions after taking appropriate safety and security measures.			Emerged through survey analises

Source: Survey validation statements (KSA) results regarding protecting personal data and privacy and final statements of DigComp 2.2 at Vuorikari, Kluzer & Punie, 2022, p. 38.

4.3 Results protecting health and well-being

Regarding health and well-being, among the 20 statements submitted to public validation, the experts found 12 statements relating to the digital health behaviour (KSA), which were crucial in preventing citizens from neglecting aspects of their digital health data. Nevertheless, even though all 12 statements selected, five of them (n=5) were not included in the DigComp 2.2 (see table 5)

Table 4. Examples of final knowledge and attitudes related with digital health for digital competence 4.3 - protecting health and wellbeing presented in the survey validation and were reframed or excluded of the DigComp framework 2.2

	Dimension 4		Decision		
Type	**Nr. Stat.**	**Statement**	**Included**	**Not Included**	**Included with Arrangements**
Knowledge	1	Aware of the importance of healthy personal digital balance regarding the use of digital technologies, including non-use as an option. Many different factors in digital life can impact on personal health, well-being and life satisfaction.			X
	2	Knows that some AI-driven applications on digital devices (sensors, wearables, smart phones) can support the adoption of healthy behaviours through monitoring and alerting about health conditions (physical, emotional, psychological). However, decisions proposed could also have potential negative impacts on physical or mental health.			X
	3	Knows that for many digital health applications, there are no official licensing procedures like is the case in classical medicine.		X	
	9	Aware that digital upskilling can create access to education and training as well as to job opportunities thus promoting social inclusion.		X	
	2	Able to gather information about digital self-help health applications for improving physical and/or mental well-being (positive and negative effects) before deciding whether to use them or not.			X
	3	Knows how to recognise embedded user experience techniques designed to be manipulative and/or to weaken one's ability to be in control of decisions (make users to spend more time on online activities, encourage consumerism).	X		
	6	Able to decide whether to deal with an online problem situation alone or to recruit professional or informal help.		X	
	7	Can select digital content and solutions that enhance usability and user engagement, choses culturally relevant content in local languages, easy to access material for low-literate users, and applies captions for videos.		X	
Attitudes	1	Assumes responsibility for protecting personal and collective health and safety when evaluating the effects of medical products and services online as there are dangers in trusting and sharing false information on health.	X		
	2	Inclined to focus on physical and mental well-being and avoid negative impact of digital media such as overuse, addiction, compulsive behaviour.	X		
	3	Wary of the reliability of recommendation (are they by a reputable source in healthcare/well-being) and their intentions (do they really help the user vs. encourage use the device more to be exposed to advertising).	X		
	4	Being willing not to harm others online.		X	

Source: Survey validation statements (knowledge and attitudes) results regarding protecting personal data and privacy and final statements of DigComp 2.2 at Vuorikari, Kluzer & Punie, 2022, p. 40.

5 Conclusion

This paper has considered critically the AI implications for health, security, and wellbeing, drawing from the body of work created by the digital safety and security working group. The working group followed the DBR as advocated by McKenney and Reeves (2014), a widely used methodology in the learning sciences to analyse the development of solutions, and this enabled the generation of ideas from the expert group, for these to be refined and distilled to the essential components of Knowledge Skills and Attitudes (KSA) as required by the EU DigComp team. The key benefit of the process was the gathering of an extensive evidence base to inform the final recommendations, and although not all were included in the revised version, the gaps in knowledge have been articulated and identified for further work. Those embedded within the new framework form the basis for educating and safeguarding EU citizens as they start to take advantage of huge changes in the way health services will be offered in future and promote a more critical engagement with digital health provision. Future work on this thematic need to replicate this research base model, and analyze the consensus proposed by the community of experts, to help citizens to take informed decisions regarding their security health and wellbeing on AI apps. The important data collected (KSA) need to be disseminated throughout academic, social, and professional contexts to empower citizens to interact on the increasing digital health apps environments.

References

Chang, A. (2020). The role of artificial intelligence in digital health. In S. Wulfovich & A. Meyers (Eds.). *Digital health entrepreneurship* (pp. 71-81). Cham: Springer.

Center for Open Data Enterprise (2019). *CODE, Sharing and utilizing health data for AI applications*. Washington, DC: Center for Open Data Enterprise.

Ferrari, A. (2012). Digital competence in practice: An analysis of frameworks. European Commission.

Ferrari, A. (2013). *DigComp: A framework for developing and understanding digital competence in Europe.* European Commission.

Fornasier, M. de O. (2021). The use of AI in digital health services and privacy regulation in GDPR and LGPD between revolution and (dis)respect. *RIL Brasília*, 59 (233), 201-220.

Goldsmith, B., Holley, D., & Quinney, A. (2020). The best way of promoting digital wellbeing in HE?, https://lmutake5.wordpress.com/2020/09/24/take5-47-the-best-way-of-promoting-digital-wellbeing-in-he/

McKenney, S., Reeves, T.C. (2014). Educational Design Research. In: J. Spector, M. Merrill, J., Elen, & M. Bishop (Eds.), Handbook of Research on Educational Communications and Technology. New York, NY: Springer.

Murdoch, B. (2021). Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics*, 22(122), 1-5.

Plomp, T. (2013). Educational design research: An introduction. In T. Plomp & N. Nienke (Eds.), *Educational design research: Part A: An introduction* (pp. 10–51). Enschede: SLO - Netherlands Institute for Curriculum Development.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad K. R. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, 8 (2), 2227-9032.

Singh, A. K., Anand, A., Lv, Z., Ko, H., & Mohan, A. (2021). A survey on healthcare data: a security perspective. *ACM Transactions on Multimidia Computing Communications and Applications*, 17(2), 1-26.

Tuckman, B. W. (2012). *Manual de investigação em educação: Metodologia para conceber e realizar o processo de investigação científica*. Lisboa: Fundação Calouste Gulbenkian.

Vuorikari. R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The digital competence framework for citizens with new examples of knowledge, skills and attitudes. European Commission.