https://doi.org/10.1038/s41591-022-02167-6

Characterizing cyber harms from digital health

Eric D. Perakslis, Megan L. Ranney & Jennifer C. Goldsack

The expansion of digital health comes with benefits, but also potential harms, including those to economic, psychological and societal wellbeing. This article presents a framework to characterize cyber harms so that they can be prevented and mitigated.

The adoption of telehealth, decentralized clinical trials, distributed care delivery, at-home diagnostic testing and personalized digital therapeutics continues to accelerate. These digital solutions are being deployed across an increasing number of health issues, ranging from reproductive health and mental health to cancer screening and diabetes. Concurrently, the incidence, cost and time to recovery of healthcare cyberattacks and data breaches have risen substantially. In the United States in 2020 alone, 599 cyberattacks affected more than 26,435,000 patients and cost an average of $499 per breached record; each breach took an average of 263 days to recover[1]. Other examples of cyber health harms include those caused by the COVID-19 infodemic, misuses of unconsented health data (such as the unconsented sale of data captured by the National Suicide Hotline in the US)[2], negative financial and emotional impacts from cybercrime, nation-state-sponsored disruption of healthcare (such as the disruption of the UK's National Health Service by WannaCry) and the use of stalkerware for intimate partner violence[3,4]. Yet these potential harms are rarely discussed or prevented.

A risk framework, developed from other commonly accepted risk frameworks, is needed to classify, identify and encourage mitigation of cyber harms within the context of rapidly evolving risks of digital health.

One of the best-characterized domains of patient safety and benefit–risk analysis is drug side effects. The pharmaceutical and medical device domains have served as the basis for the US Food and Drug Administration's consideration of digital health validation and provide an exemplar for understanding risks from digital health. Drug side effects are often classified therapeutically, but can instead be organized anatomically, in an easily understood hierarchical matrix of organ systems, organs and severity of known side effects[5]. The field of cybersecurity has recently produced an analogous classification system for cyber harms that can be adapted to digital health[6], whereby internet connectivity results in increased risks as exposure to the internet increases, not unlike incidence proportion in classical epidemiology[7]. Cyber harm is a new health risk in the digital era of health, along with misdiagnosis, mistreatment, misinformation, cyberchondria and poor health outcomes, which cascade from inadequately secured systems and exploited data.

Digital health vulnerabilities

The first step in constructing a risk framework for digital health is to understand the vulnerabilities relevant to the populations of interest. Table 1 describes potential digital health vulnerabilities according to the five dimensions of the taxonomy of cyber harms. Just as health outcomes are inextricably linked to social factors, so are digital health risk factors; these factors can interact and thereby increase or decrease the relative benefit or harm[8]. Considering these vulnerabilities is critical to protecting patients by increasing equity of benefit and decreasing harms.

Table 1 | Risk factors for digital health harms[6,11]

Vulnerability	Examples of risk factors
Physical/digital	Shared residences such as shelters and hotels Lack of secure WiFi Outdated mobile technology Lack of regulation regarding data-sharing
Economic	Low socioeconomic status Unemployment Lack of high school diploma
Psychological	Multiple chronic conditions Mental illness Dementia Substance use disorder Young or old age Frequent social media use
Reputational	Frequent social media use Low digital literacy Low health literacy Young or old age Immigration status Stigmatized illnesses
Societal	Geography Local policies Minority status Immigration status Non-English-speaking status Physical disability Young or old age

For example, a family that cannot afford home broadband service might rely on public WiFi to access a patient portal, thereby increasing the probability of identity theft and exacerbating their preexisting financial vulnerability. Low digital or health literacy increases the chance of stolen data and of vulnerability to health misinformation. Loss of reproductive privacy can now lead to criminal charges in the United States for patients and clinicians[9], with geography the greatest risk factor. Many US states that have or are in the process of outlawing abortion have some of the highest Social Vulnerability Index scores[10,11]. The primary categories of this proposed model therefore include harms in the physical/digital, economic, psychological, reputational and societal domains.

Cyber harms

The second step in the framework is to codify the potential harms that can result from these digital health vulnerabilities. Codifying harms from technologies can be difficult and complex, and should not be read as a blanket condemnation of digital health. For example, there are many virtuous and valuable uses for health-related social media

Table 2 | Case studies of digital health harms and potential mitigating strategies

Example of harm	Technical vector (2020 incidence)	Regulator/enforcement (US)	Assessment framework or case study	Further reading
Intimate partner violence	Stalkerware (up 780%)	FTC, law enforcement	The Danger Assessment	Freed, D. et al.
Care disruption	Cyberattack (up 141%)	HHS, DHS, law enforcement	Baby Kidd	Perakslis, E.
Identity theft	Malware (up 100%)	HHS, FTC, law enforcement	Carlos from San Antonio	Federal Trade Commission
Loss of employment or underemployment	Stolen data (33% of victims)	DoJ, but unclear	Alexis Moore	Identity Theft Resource Network
Fraud and tax burden	Stolen data	IRS, FTC	Tax consequences of identity theft	Taxpayer Advocate Service
Criminal record	Physically stolen data for fraud	HHS, DoJ, law enforcement	Deborah Ford	HHS OIG
Loss of reproductive privacy	Data brokers	HHS, FTC, but unclear	32 brokers selling billions of profiles	Al Ghadeer, H.A. et al.
Post-traumatic stress and/or depression	Secondary (86% of victims)	N/A	Ashley Madison suicides	State of Georgia
Radicalization	Social media/digital engagement	FTC, FCC, DHS	Peyton Gendron	Von Behr, I. et al.

DHS, Department of Homeland Security; DoJ, Department of Justice; FCC, Federal Communications Commission; FTC, Federal Trade Commission; HHS, Department of Health and Human Services; IRS, Internal Revenue Service; OIG, Office of Inspector General. N/A, not applicable.

campaigns. Similarly, segmenting target audiences based on digitally collected data and information can allow a precise match between potential clinical trial participants and potentially lifesaving investigational therapies. Unfortunately, these same tools can also be utilized to disseminate disinformation, to radicalize and manipulate people towards violence, or to initiate social engineering cyberattacks in which people are manipulated into providing data or credentials. In order for the healthcare industry to reap the benefits of digital health tools, everyone working this field must understand the ways in which digital toolsets can worsen health and exacerbate public health issues, whether these contributions are causal, contributing or benignly enabling.

Cyber harm can have major economic ramifications, such as the criminal diversion of improper Medicare payments, estimated to have cost $28 billion in the United States in 2019 alone, and cyberattacks such as those against Boston Children's Hospital in 2014 and the WannaCry ransomware attack, which crippled healthcare infrastructure[12]. Given the major impact of cyberattacks on healthcare, a Zero Trust framework is required, in which all users, whether in or outside the organization's network, need to be authenticated, authorized and continuously validated before being granted access to applications and data.

Not all digital health cyber harms are caused by criminal actors. Patients can experience mental and psychological harm if their diagnoses are inadvertently revealed by digital health companies or seen on digital devices by friends, family or third parties. Another risk is third-party selling of information, sometimes about sensitive diseases, and the potential release of information on sensitive topics such as reproductive health, which can cause major reputational harm[13–15]. For some disease entities or digital health solutions, psychological or physical harms may be more salient than systems disruptions or economic costs. Awareness of what types of harm are possible in each case can allow mitigation measures to be put in place.

Additional examples of harms are presented in Table 2; many of these are potentiated by multiple coexisting vulnerabilities[4,16–20]. The interplay is complex. Sometimes the technology is an attack vector, but in other instances, the technology may be only partially causative or contributing, with other vulnerabilities, such as the use of outdated technology or being in an abusive relationship, potentiating the cyber harm.

Table 2 also demonstrates the fragmented legal and regulatory framework for addressing cyber harms in the United States, which include law enforcement, health, media and economic regulatory agencies. Few digital health companies are 'covered entities'[21]; they are therefore not subject to the minimal protections afforded by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These gaps in legal protections leave vulnerable patients at higher risk than the less vulnerable, as those with the most serious illnesses often have the greatest exposure due to frequency of healthcare visits and diversity of facilities visited. As with polypharmacy, multiple cyber harms can occur simultaneously from a single exposure.

Although these potential harms can and have been experienced by everyone from individuals to multi-billion-dollar healthcare systems, those who are socially vulnerable are at highest risk. Minority populations and the elderly are targeted by cybercriminals more often than others, and vulnerability to various types of cybercrime is directly related to socioeconomic status[22]. Populations that are particularly vulnerable to cyber harms must be protected proportional to their risk.

Impact and likelihood

The impact and likelihood of harms from digital health technologies, and potential mitigation strategies, can be assessed using a classification framework. Table 3 proposes an evaluative approach based on a previously modified cyber risk equation that accounts for the cumulative effects of health, social and cyber vulnerabilities[23]. This framework can be applied where digital solutions might be used in clinical and clinical research situations, providing a useful guide for digital health developers and healthcare providers alike. The framework emphasizes the importance of social and physical vulnerabilities. It also highlights that one can reduce the risk of harm in multiple ways: by minimizing

Table 3 | Evaluation framework for harms from digital health interventions

	Threat: any event that causes loss of data confidentiality, integrity or availability	Example patient	Attack surface: summation of points on the boundaries of a system where an attacker can enter or attack	Vulnerabilities of:		Impact: potential damage caused by an event	Likelihood: chance of an attack	Potential mitigation strategies: examples of physical, procedural and technical controls that reduce impact and likelihood
				Technologies	Patient populations (physical/digital, economic, psychological, reputational and/or societal vulnerabilities)			
Patients newly diagnosed with MS enrolling in a clinical trial	Enrolment in a clinical trial poses a cyber threat, as it requires actigraphy, sleep monitoring and patient-reported outcomes data on activities of daily living.	**Patient A**	**High:** Activity and diet closely tracked using internet-accessed technology	**Low:** Patient has purchased high-end devices including the latest smartwatch and iOS phone and a company-provided secure VPN in the home.	**Low:** Recent diagnosis and strong employment, with a hybrid work schedule. Patient is well educated, works in financial technology and is highly tech literate.	**Low:** If information is used, it has low reputational risk to patient, and patient has the education and means to minimize cyber harm.	**Low:** Patient has multiple protective measures and potential mitigation strategies in place.	**Physical/digital:** Give patient the cellphone or smart watch for the trial. Encourage uploading of data only on private WiFi. **Economic:** Provide a year of identity theft protection and credit counseling. **Reputational:** Provide personal 'cyber-hygiene' training at time of enrollment.
		Patient B	**High:** Activity and diet closely tracked using internet-accessed technology	**High:** Patient has low-end, older devices and uses public WiFi to connect to the study.	**Moderate:** Recent diagnosis and good employment history, but patient does not track credit scores and has previously fallen for phishing scams.	**Moderate–high:** If information is used, it has low reputational risk to patient, but patient lacks the education and means to minimize cyber harm.	**Moderate:** Patient lacks multiple protective measures and mitigation strategies.	
Patient seeking reproductive healthcare	Use of a period-tracking app to reduce risk of pregnancy	**Patient A**	**Low:** Use of a single app	**High:** App shares data with third-party services. The data live on a cloud server and cannot be fully deleted by the user.	**High:** Patient is a victim of partner violence. Additionally, they live in a state with restrictions on access to abortion.	**High:** A data leak would put patient at risk of both increased violence and legal harm (given state policies).	**High:** Program shares data without consent. Patient also has multiple personal and societal vulnerabilities and no mitigation measures.	**Physical/digital:** Register for the app anonymously. Use apps with local, not cloud-based, storage of data. **Economic:** Legislation prohibiting non-consented selling or reidentification of anonymized health data. **Psychological:** Find safe online communities outside commercial digital health products. **Reputational:** Ensure location tracking is off on all apps on mobile devices. Do not use transportation apps, such as Uber or Lyft for reproductive health appointments. **Societal:** Change policies around reproductive healthcare access.
		Patient B	**Low:** Use of a single app	**Moderate:** App recently changed security settings to allow anonymous use. However, the data live on a cloud server and cannot be fully deleted.	**Low:** Patient lives in a state with no restrictions on reproductive healthcare, has secure employment and has a healthy relationship with their partner.	**Low:** Even if data were leaked, patient would experience no personal consequences.	**Low:** Patient uses the most secure version of the app and has few vulnerabilities.	

the attack surface, minimizing vulnerabilities or incorporating other mitigation measures.

The intention of this framework, like that of the US Food and Drug Administration's pharmaceutical framework[5], is not to dissuade use of digital health, but rather to focus attention on the importance of identifying, and mitigating, potential harms for the populations that are most at risk. To ensure the safety of patients in the digital era of health, those advancing digital strategies must study and classify the cyber side effects of digital health and build accurate and proportional benefit–risk frameworks to guide essential innovations. Proactively mitigating risk will make the benefits of digital health more likely to be realized by the full spectrum of patients and healthcare systems.

More focused, aligned and actionable regulatory frameworks that close the gaps between federal regulators and law enforcement are required as an effective deterrent to bad actors. When crime carries extremely low risk of consequence, it flourishes, but there are mitigations available today that should be utilized.

Finally, the most important step may be the easiest. In digital health, simply being thoughtful about when and why digital tools and datasets are connected to the internet can dramatically decrease risk, as demonstrated in Table 3. It is impossible to eradicate risk altogether, but an intentional approach can successfully identify when and where risks of harm exists, indicate the most successful mitigation strategies and ensure that the benefits of the digitization of healthcare can be reaped by all individuals the healthcare system is intended to serve.

Eric D. Perakslis[1,2], Megan L. Ranney[3,4] ✉ & Jennifer C. Goldsack[5]
[1]Duke Clinical Research Institute, Duke University, Durham, NC, USA. [2]Department of Population Health Sciences, Duke University School of Medicine, Durham, NC, USA. [3]Brown-Lifespan Center for Digital Health, Providence, RI, USA. [4]School of Public Health, Brown University, Providence, RI, USA. [5]Digital Medicine Society, Boston, MA, USA.
✉e-mail: megan_ranney@brown.edu

Published online: 9 February 2023

References

1. Healthcare Breach Report 2021: Hacking and IT Incidents on the Rise (Bitglass, 2021); https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q1HealthcareBreachReport2021.pdf
2. Levine, A. S. *Politico* https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617 (2022).
3. Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J. & Hutton, S. *J. Forensic Sci.* **49**, 131–136 (2004).
4. Scroxton, A. *ComputerWeekly.com* https://www.computerweekly.com/news/252492575/Use-of-abusive-stalkerware-against-women-skyrocketed-in-2020 (2020).
5. Wadhwa, S., Gupta, A., Dokania, S., Kanji, R. & Bagler, G. *PLOS One* **13**, e0193959 (2020).
6. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. & Upton, D. *J. Cybersecurity* **4**, tyy006 (2018).
7. US Centers for Disease Control. Measures of Risk (CDC, 2012); https://www.cdc.gov/csels/dsepd/ss1978/lesson3/section2.html
8. Thornton, R. L. J. et al. *Health Aff.* **35**, 1416–1423 (2019).
9. Yao, K. & Ranney, M. L. *CNN.org* https://www.cnn.com/2022/06/16/opinions/period-trackers-app-roe-abortion-ranney-yao (2022).
10. Messerly, M. *Politico.com* https://www.politico.com/news/2022/06/24/abortion-laws-by-state-roe-v-wade-00037695 (2022).
11. Agency for Toxic Substances and Disease Registry (ATSDR), CDC. Social Vulnerability Index (2022); https://www.atsdr.cdc.gov/placeandhealth/svi/index.html
12. US Centers for Medicare & Medicaid Service. 2019 Estimated Improper Payment Rates for Centers for Medicare & Medicaid Services (CMS) Programs (2019); https://www.cms.gov/newsroom/fact-sheets/2019-estimated-improper-payment-rates-centers-medicare-medicaid-services-cms-programs
13. Hamideh, D. & Nebeker, C. *Curr. Addict. Rep.* **7**, 317–332 (2020).
14. Grundy, Q. et al. *BMJ* **364**, l920 (2019).
15. Schaffer, A., Marks, J. & Knowles, H. P. *Washington Post* https://www.washingtonpost.com/nation/2021/12/01/los-angeles-planned-parenthood-hack/ (2021).
16. Whitney, L. 2020 sees huge increase in records exposed in data breaches. *TechRepublic* https://www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/ (2021).
17. Skiba, K. Pandemic proves to be fertile ground for identity thieves. AARP (2021); https://www.aarp.org/money/scams-fraud/info-2021/ftc-fraud-report-identity-theft-pandemic.html
18. Guynn, J. *USA Today* https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/ (2020).
19. Kelley, T. F. *J. Media Eth.* **37**, 141–150 (2022).
20. Grant, K. *CNBC.com* https://www.cnbc.com/2019/01/07/how-identity-theft-causes-problems-at-work.html (2019).
21. US Department of Health and Human Services. Covered Entities and Business Associates (HHS, 2017); https://www.hhs.gov/hipaa/for-p.rofessionals/covered-entities/index.html
22. Seals, T. Women, minorities are hacked more than others. Threatpost.com (2021); https://threatpost.com/women-minorities-hacked/175038/
23. Perakslis, E. & Stanley, M. *Digital Health: Understanding the Benefit-Risk Patient-Provider Framework* (Oxford Univ. Press, 2021).

Competing interests

The authors declare no competing interests.