Original Article

Healthc Inform Res. 2022 April;28(2):132-142.
https://doi.org/10.4258/hir.2022.28.2.132
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records

Nehama Lewis[1], Yaron Connelly[2,3], Gil Henkin[4], Max Leibovich[4], Adi Akavia[4]

[1]Department of Communication, University of Haifa, Haifa, Israel
[2]Department of Sociology, University of Haifa, Haifa, Israel
[3]The Israeli Center for Emerging Technologies (ICET), Shamir Medical Center, Zerifin, Israel
[4]Department of Computer Science, University of Haifa, Haifa, Israel

Objectives: Healthcare organizations that maintain and process Electronic Medical Records are at risk of cyber-attacks, which can lead to breaches of confidentiality, financial harm, and possible interference with medical care. State-of-the-art methods in cryptography have the potential to offer improved security of medical records; nonetheless, healthcare providers may be reluctant to adopt and implement them. The objectives of this study were to assess current data management and security procedures; to identify attitudes, knowledge, perceived norms, and self-efficacy regarding the adoption of advanced cryptographic techniques; and to offer guidelines that could help policy-makers and data security professionals work together to ensure that patient data are both secure and accessible. **Methods:** We conducted 12 in-depth semi-structured interviews with managers and individuals in key cybersecurity positions within Israeli healthcare organizations. The interviews assessed perceptions of the feasibility and benefits of adopting advanced cryptographic techniques for enhancing data security. Qualitative data analysis was performed using thematic network mapping. **Results:** Key data security personnel did not perceive advanced cybersecurity technologies to be a high priority for funding or adoption within their organizations. We identified three major barriers to the adoption of advanced cryptographic technologies for information security: barriers associated with regulators; barriers associated with healthcare providers; and barriers associated with the vendors that develop cybersecurity systems. **Conclusions:** We suggest guidelines that may enhance patient data security within the healthcare system and reduce the risk of future data breaches by facilitating cross-sectoral collaboration within the healthcare ecosystem.

Keywords: Information Science, Computer Security, Medical Records, Data Protection, Interview

Submitted: May 31, 2021
Revised: 1st, December 30, 2021; 2nd, February 28, 2022
Accepted: March 1, 2022

Corresponding Author
Yaron Connelly
The Israeli Center for Emerging Technologies (ICET), Shamir Medical Center, Zerifin 703301, Israel. Tel: +972-542254452, E-mail: Yaron.Connelly@gmail.com (https://orcid.org/0000-0002-7924-9663)

I. Introduction

In the last decade, healthcare organizations (i.e., clinics and hospitals) have been increasingly moving toward online data aggregation of patient medical records using cloud computing and other storage methods [1]. In recent years, the use of Internet of Things (IoT) technology in healthcare has increased, and online data and communication have also been used for operating medical devices [2]. The collection and storage of medical data may exceed the boundaries of organizations and be carried out by states, as occurred during the coronavirus disease 2019 (COVID-19) pandemic [3]. The use of computerized data can increase the efficiency of patient care. However, like other personal data, this type of information is sensitive and valuable, and is thus highly vulnerable to attack by cyber-criminals [4].

The COVID-19 pandemic has highlighted the importance of securing patient data that may be insufficiently protected. In 2020, healthcare organizations around the world such as hospitals and clinics suffered from an unprecedented spike in cyber-attacks [5,6]. In 2020, more than 400 organizations and 20 million individuals were affected in the United States healthcare system alone [7]. Well-known attacks have also occurred in the recent past, before the COVID-19 pandemic, including the May 2017 coordinated ransomware attack (WannaCry) that affected more than 200,000 devices in more than 150 countries, including the United Kingdom's National Health Service, resulting in mass chaos and the suspension of health services in many locations. In addition to their financial threats, cyber-attacks could result in patient mortality if care is disrupted [8]. No country is immune to these threats, and national regulatory bodies must allocate the resources and means to protect against these attacks [6].

Advances in cryptographic data protection [9] have the potential to improve the security of medical records by providing not only a perimeter defense against attacks from outside the organization, but also an ongoing defense against both external and in-house attacks. This is achieved by storing the data in an encrypted or masked form, so that even if an attacker breaks the perimeter defense to infiltrate the system, they will not compromise data security. Using state-of-the-art methods in cryptography, such a defense is feasible not only for data-at-rest but also for data-in-use [10-13].

While there is a clear need to invest in new approaches and to develop policies that will increase the security of medical data, healthcare providers may be reluctant to adopt and utilize the most advanced cybersecurity technologies available. At the organizational level, cybersecurity can be seen as essential but expensive [14], particularly in organizations with limited resources. At the operational level, staff members might consider cybersecurity to be a burden or an interruption to their workflow and to patient care [15]. Healthcare management may also be cognizant of the need to allow continuous access to patient data among their medical and administrative staff, including remote access by physicians [16]. However, few studies have examined factors that may account for the willingness to adopt future innovative cybersecurity techniques within the healthcare sector.

This paper describes a qualitative study of data collected through a series of interviews with key cyber-protection stakeholders in the Israeli healthcare system. The Israeli healthcare infrastructure, which is under threat of cyber-attack, consists of 33 major hospitals, four major research institutes, and four health maintenance organization (HMO) networks with about 2,500 community health clinics. In 2017, cyberattacks targeting four Israeli hospitals were successfully deflected [17]. However, in October 2021, a massive ransomware attack on a public hospital did breach the system, paralyzing the majority of the hospital's computer systems [18]; the hospital refused to pay the ransom and re-established its information systems in 52 days, when eventually all patients' medical information was restored and no patient data was leaked [19]. In the years leading up to the cyber-events, Israeli policymakers have worked to promote the digitization of medical records, organizational databases, and a national shared network of medical data [20]. Several entities have been established in these years to address the emerging regulatory cyber-challenges (the National Cyber System, the Privacy Protection Authority and the Digital Health and Computing Division of the Ministry of Health). However, the Israeli health sector may not be adequately prepared for the risk of cyber-threats against national healthcare critical infrastructure, and a comprehensive law for cyber-protection in Israel is currently only in the drafting stage [21].

The aims of this study were (1) to assess current data management and security procedures and perceptions of vulnerability to cyber-attacks, and (2) to identify attitudes (perceived risks and benefits/usefulness), knowledge, perceived norms, and self-efficacy with regard to the adoption of advanced cryptographic techniques. These constructs are drawn from well-established behavioral theories such as the technology acceptance model [22], the theory of planned behavior [23], and protection motivation theory [24]. These theories have been used to explain variation in the adoption of technological practices and products in prior research [15,22]. The aims of this study were addressed through an analysis of data elicited via interviews assessing participants' perceptions and attitudes. Finally, we offer guidelines that could help policymakers and data security professionals work together to ensure that the patient data is secure but also accessible. The suggested guidelines are described in Section IV, where we provide an interpretive analysis of the study's findings and offer practical guidelines based on the results.

II. Methods

1. Study Design

We applied a naturalistic approach in this qualitative study to design and conduct 12 in-depth semi-structured interviews with the proposed group of data security managers and individuals in key cybersecurity positions within Israeli healthcare organizations. Based on the framework suggested by Guba and Lincoln [25], four criteria were considered for maintaining the trustworthiness of our study throughout all its stages as detailed below: credibility, transferability, dependability, and confirmability [26].

The interview protocol (Appendix 1) included questions addressing: (1) technological aspects, with an emphasis on cryptographic technologies; (2) organizational aspects, with an emphasis on the Israeli healthcare ecosystem; and (3) psychosocial aspects, with an emphasis on understanding the respondents' perceived benefits and costs of alternative methods of patient data security, their willingness to adopt innovative cryptographic methods, and (perceived and actual) obstacles to adoption.

2. Participants

In order to create purposive sampling of key cybersecurity positions in the Israeli health system, an online search engine (Google) was systematically queried. The search strategy included a combination of keywords under two predetermined inclusion criteria: (1) healthcare institute or organization name (e.g., Clalit Health Services or Tel Aviv Sourasky Medical Center) and (2) name of the key position or senior job description (e.g., CIO or Head of division + Cybersecurity). The search identified 25 names of potential participants who were invited to take part in the study, of whom 12 participants (10 men and two women) from seven Israeli healthcare organizations accepted the invitation and volunteered to be interviewed. All participants held a senior position in their organization and had over 10 years of employment experience that included several positions in the fields of cybersecurity or information security, focused on the healthcare domain. Most participants were aged between 40 and 55.

Table 1 provides participants' specialty, position, and the type of organization they represented, which are important data for understanding the possible transferability of this study, which refers to the degree to which qualitative data for a unique case is based on a broad representation [25,26]. As can be seen in Table 1, the sample of participants represented several types of sites (organizations) and several types of positions (interviewees), all of which are part of the healthcare system.

3. Data Collection

Potential participants were invited via email to participate in a 60-minute interview, noting that all collected data would be stripped of identifying details. The invitation included information about the research objectives, funding organization, and the principal investigators. The recruitment phase was carried out between January and March 2019. The research team members conducted face-to-face interviews over a 1-year period (May 2019 to May 2020) at the partici-

Table 1. Participants' information (n = 12)

	Specialty	Position	Type of organization
1	Information systems	Head of division/department	Research center/institute
2	Information systems	IT administrator	Research center/institute
3	Information systems	CIO	Public hospital (number of beds >1,000)
4	Information systems	CIO	Public hospital (number of beds >1,000)
5	Information systems	CIO	Public hospital (number of beds <1,000)
6	Information systems	CIO	HMO hospital (number of beds <1,000)
7	Cybersecurity	Head of division/department	HMO (national provider)
8	Cybersecurity	Head of division/department	HMO hospital (number of beds <1,000)
9	Cybersecurity	Head of division/department	Public hospital (number of beds >1,000)
10	Cybersecurity	Infrastructure manager	Public hospital (number of beds >1,000)
11	Technology / Innovation	CTO	Public hospital (number of beds <1,000)
12	Technology / Innovation	Head of division	Public hospital (number of beds <1,000)

The study included 12 participants (10 men and 2 women) and most participants were aged between 40 and 55.
CIO: chief information officer, HMO: health maintenance organization, CTO: chief technology officer.

pants' place of work. Considering the interdisciplinary nature of this study and in order to strengthen the credibility of the study by researcher triangulation [25,26], the interviews were conducted by two interviewers from different backgrounds of expertise (computer science and health policy). Using the funnel approach [27], interviews began with broad questions about information and cybersecurity management within the organization and then progressed to more specific questions about their familiarity with cryptographic methods and perceptions of the necessity and willingness to adopt them. In order to strengthen the credibility of the data [25], we concluded all interviews with an understanding check. This process helps verify that the qualitative data and its interpretation by investigators are congruent with the reality as grasped by participants [25,26]. Specifically, the interviewers concluded all interviews with a summary of what they understood was said by the study participant during the interview and then asked the interviewees if their summary was correct, and whether there were any further insights that should be included in the interview.

All participants provided informed consent to be interviewed, and ethical approval was granted for this study by the Ethics Committee of the Faculty of Social Sciences at the University of Haifa (IRB No. 19/081).

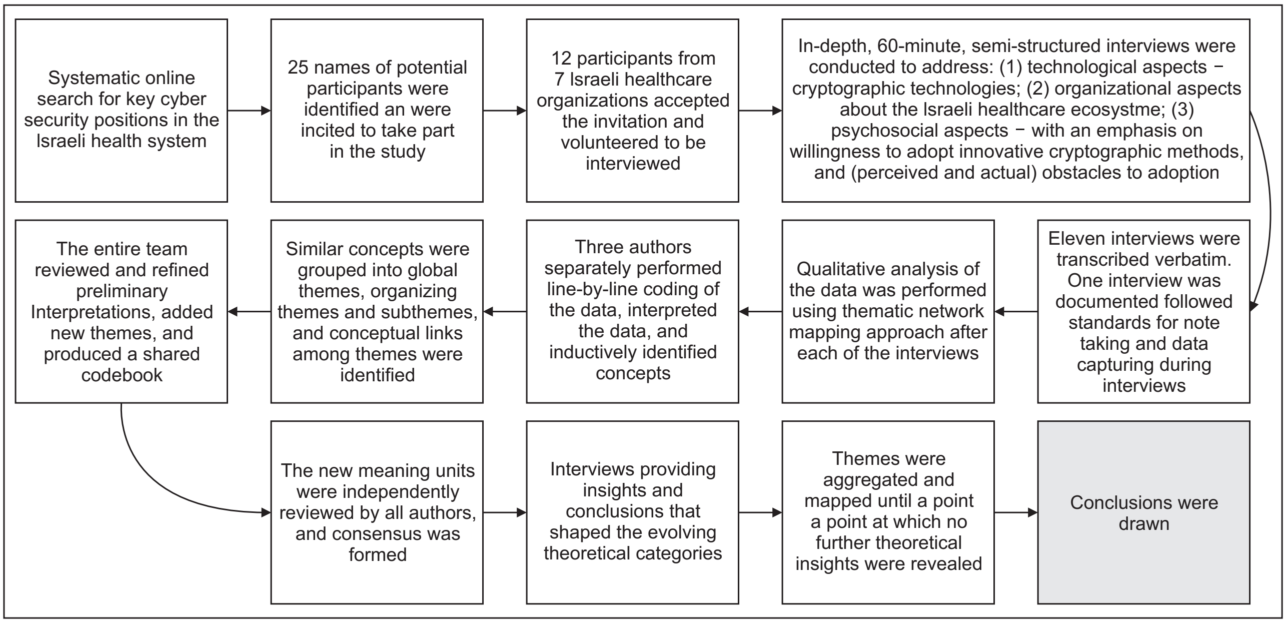
4. Data Analysis

In order to address the dependability of the study, consent to recording and full documentation of the interview was requested from all interviewees. All but one of the interviewees agreed to the documentation of the interviews, which were transcribed verbatim. The only interview not recorded was documented by the interviewers, who followed standards for taking notes and capturing data during semi-structured interviews [27]. Qualitative analysis of the data was performed using thematic network mapping [28] after each interview. First, three authors separately performed line-by-line coding of the data, interpreted the data, and inductively identified concepts. Second, similar concepts were grouped into global themes, organizing themes, and subthemes, and conceptual links among themes were identified. Third, the entire team reviewed and refined the preliminary interpretations, added new themes, and produced a shared codebook. The new meaning units were independently reviewed by all authors, and consensus was formed during team meetings. This multi-stage data analysis enabled us to ground our conclusions on interpretations from several different perspectives, strengthening the confirmability of the study [25,26]. Furthermore, following the qualitative analysis principles presented by Charmaz [29], we conducted interviews over time, and the interviews provided insights and conclusions that shaped the evolving theoretical categories. Through this process, we also reached a point at which no further theoretical insights were revealed and saturation was achieved. The flow of the study is presented step-by-step in Figure 1, which describes the process by which conclusions were drawn.

III. Results

1. Main Findings

The analysis of the interviews allowed us to address our



Systematic online search for key cyber security positions in the Israeli health system
25 names of potential participants were identified an were incited to take part in the study
12 participants from 7 Israeli healthcare organizations accepted the invitation and volunteered to be interviewed
In-depth, 60-minute, semi-structured interviews were conducted to address: (1) technological aspects − cryptographic technologies; (2) organizational aspects about the Israeli healthcare ecosystme; (3) psychosocial aspects − with an emphasis on willingness to adopt innovative cryptographic methods, and (perceived and actual) obstacles to adoption
Eleven interviews were transcribed verbatim. One interview was documented followed standards for note taking and data capturing during interviews
Qualitative analysis of the data was performed using thematic network mapping approach after each of the interviews
Three authors separately performed line-by-line coding of the data, interpreted the data, and inductively identified concepts
Similar concepts were grouped into global themes, organizing themes and subthemes, and conceptual links among themes were identified
The entire team reviewed and refined preliminary Interpretations, added new themes, and produced a shared codebook
The new meaning units were independently reviewed by all authors, and consensus was formed
Interviews providing insights and conclusions that shaped the evolving theoretical categories
Themes were aggregated and mapped until a point a point at which no further theoretical insights were revealed
Conclusions were drawn

Figure 1. Qualitative study flow.

first two study aims (i.e., to assess current perceptions and attitudes). The findings indicated that participants in key data security positions did not believe that highly advanced cybersecurity is, or should be, a high priority for funding or adoption in their organization. Table 2 summarizes the theme mapping of this study. We identified three major barriers to the adoption of advanced cryptographic technologies for information security: (1) barriers associated with regulators; (2) barriers associated with healthcare providers (including organizations such as hospitals and HMOs and individuals such as medical staff); and (3) barriers associated with the vendors that develop and market cybersecurity systems.

2. Themes

1) Barriers associated with regulators

Most participants felt that the data security regulations with which they must comply were not aligned with the reality of data security in healthcare. Participants noted that regulatory standards were imprecise, often impossible to comply with in practice, and did not provide clear guidelines for application. Without clear and explicit regulatory standards, respondents expressed reluctance to petition for additional resources for upgrading security infrastructure.

(1) Vague standards: "Drafts are issued and then stay at the draft level for two or three years, because there are a lot of questions raised that are never resolved. On the other hand, even when it [the draft] eventually comes out as a regulation—enforcement is not even at the minimum level, which results in everyone doing whatever they want."

(2) Lack of regulation: "The lack of regulation in our field is well known. The difficulties that information security faces in the medical world are endless because there are not enough resources… because there is no one that forces our management or the Ministry of Health to provide these resources… Suppose I now ask my management for a new million-dollar system. They will look at me – 'What do you want from us? Where is it written that we need this?'"

(3) Unrealistic regulations: "It is not wise to impose regulations without providing resources, just as it's not smart to tell me to do something that I have no chance of doing. Look, for example, the regulator says all computers have to have Windows 10. Okay, but we have an OCT machine for eye photography with XP. You cannot fulfill the regulation! Replacing all devices according to the regulation would cost millions, and 'It does not work that way.'"

2) Barriers associated with healthcare providers

Participants perceived the healthcare environment as dy-

Table 2. Theme mapping

Factor	Theme code	Description
Factors associated with regulators	1	Data security regulations are not aligned with the reality of data security in healthcare.
Vague standards	1.1	Drafts are issued and then remain at the draft level for two or more years.
Lack of regulation	1.2	If there is no explicit requirement that data security must be implemented, it is unlikely to be adopted voluntarily by management.
Unrealistic regulations	1.3	Regulations that are imposed without necessary resources are not effective and will not be implemented.
Factors associated with healthcare providers	2	Healthcare institutions require balancing a commitment to patient data protection alongside organizational demands for efficient patient care and service.
Low capacity	2.1	There is a need to balance continually increasing costs of cybersecurity in a context of limited resources.
Business priorities	2.2	Patient data security is not seen as a high priority within the organizations
An uninterrupted workflow	2.3	There are concerns that excessive security might hinder the optimal workflow of the professional staff.
A responsive approach	2.4	Most participants adopted a responsive approach toward decision making with regard to cyber-threats, rather than a preventative approach.
Factors associated with vendors	3	Participants discussed the cyber-defense systems they use on a daily basis as products that are expected to provide them added value.
Unclear return on investment (ROI)/ necessity	3.1	Participants expressed skepticism about the claim that cryptographic methods of cybersecurity would provide significant added value relative to the current infrastructures.

namic, complex, and characterized by constraints that require balancing a commitment to patient data protection alongside organizational demands for efficient patient care and service, particularly the need to ensure continual access to patient data by the professional staff.

(1) Low capacity: Participants acknowledged the difficulties posed by the continually rising costs of cybersecurity when the resources available to them are very limited, in terms of both budget and professional human capital. They cited this tension as an obstacle to upgrading their security systems.

"Lack of resources also causes employee burnout. The existing resources are people… I'm not buying new systems anymore, because I can't afford it with my existing resources [small number of employees]."

"Today I need to protect more and more vectors…the whole IoT world is coming in so I need to protect that as well…. I mean, it's no longer just IT and medical devices. We have more vectors to protect but much lower budgets."

(2) Business priorities: Some participants assessed that information security was not seen as a high priority in their organization. They believed that their organization prioritized resource allocation toward core healthcare activities rather than toward investing in data security infrastructure.

"I remind you that the hospital's business is to provide care. One more PET-CT machine is more important than any of the organization's cybersecurity. That is a risk assessment, at the economic level for sure."

"One should always look at two aspects: information systems usually deal with the technological side, and the business management always looks at the business interest. Somehow information security was created to link business to technology, it is about balances, because there are limited resources."

(3) The importance of an uninterrupted workflow: Several participants perceived there to be a tradeoff between data security and access, when excessive security might hinder the optimal workflow of the professional staff. Several participants (computer and information security professionals) felt that ensuring employees' ability to access patient data was vital, even at the cost of less stringent security protocols.

"We are enablers, not preventers. We manage permissions for users who need them for various applications and systems... give access and not deny access. Doctors are not here 24/7... If we need their advice, it is necessary that they access the patient's record remotely. The access is managed according to the guidelines set by the Ministry of Health and those we set ourselves."

"I'll tell you where it becomes a problem. Suddenly some of our users cannot work properly and then you have to start chasing an information security team that does not understand where the problem is. You have to call 30 people trying to understand who made the change that now affects you..."

(4) A responsive approach: Another recurring theme in our analysis was the participants' approach to decision-making. Most participants in our study adopted a responsive approach to decision-making with regard to cyber-threats, rather than a preventative approach by investing resources in cyber-defense to mitigate future risks.

"Unfortunately, in the world of cybersecurity, as long as everything is fine then the management does not really see any need beyond a reasonable level. In May 2017, there was an attack on the world of healthcare. The management said: 'We were not hurt? Ok. Next!' Not every attack that hits someone else shocks them."

"If someone were to ask for an extra budget for pandemic diseases in 2019, then they probably would not get a penny. The same also goes for cybersecurity. If there is a major event here, maybe even if people get hurt, then there is no doubt that everyone will wake up."

3) Barriers associated with vendors

Participants discussed the cyber-defense systems they use on a daily basis as products that are expected to provide added value. When vendors fail to prove added value, there is a reduced likelihood that organizations will invest in the advanced cryptographic security systems that they offer.

(1) Unclear return on investment (ROI)/necessity: Some participants were skeptical about claims that cryptographic methods of cybersecurity would provide them with significant added value relative to the infrastructure they currently use.

"I think we would use existing tools and would not mess with it for now (cryptographic technology)… First, we look for added value."

"It is difficult to prove the direct and immediate link between information security and ROI because it does not exist. The ROI that comes from information security is very long-term. This is risk minimization and not something that can be quantified in real money."

IV. Discussion

This qualitative study examined the attitudes of individuals occupying key positions in cybersecurity and information security towards adopting advanced cryptographic methods for enhanced data protection in healthcare. Our results indicate that the Israeli healthcare system is not yet ready to adopt this technology, and we identified several barriers in the healthcare ecosystem that can account for this. The third aim of the study was to offer guidelines that could assist policy-makers and data security professionals in working together via an interpretive analysis of the findings. Indeed, we found that the results can offer new insights into the relationships between actors involved in patient data protection—healthcare providers, regulatory bodies, and the technological sector. It is noteworthy that most of the interviews were conducted before the COVID-19 pandemic, while others were conducted during the early stages of the pandemic. However, we did not identify differences in the themes raised by different interviewees according to the timing of the interviews.

The results of this study point to several implications and recommendations for enhancing patient data security within the Israeli healthcare system and reducing the risk of future data breaches.

1. COVID-19: A Call for Integration against Growing Threats

The COVID-19 pandemic has raised critical questions regarding how healthcare organizations and countries can and should protect patient data at a time when healthcare infrastructure is a particularly significant target for attackers. These questions involve stakeholders across multiple sectors—policy-makers, healthcare professionals, data security experts, the technological sector, and the public. The study findings reflect a responsive rather than a proactive approach towards cyber-threats in the healthcare field. However, at present, a breach of patient data of the type that has already occurred [18,19] may exact an even more devastating price than ever before. For example, patient data will now include patients' history of COVID-19 infection and vaccinations. These data are highly sensitive. The process by which these data are collected, stored and shared will have widespread social, political, and economic implications. There is an urgent need for integration between stakeholders in order to develop data security policies that are clear and enforceable, but also well matched to the needs of the healthcare sector and aligned with products and technologies currently being developed in the market.

2. GDPR as a Model for Regulation

The results of this study underscore the central role of regulation as the key driving force for the adoption of enhanced security. Specifically, participants described a work environment in which regulations regarding the security of medical information are not applicable due to being unclear or unrealistic. Regulation provides a policy framework for evaluating and updating cybersecurity strategies and defining objectives at the national level. Yet, a comprehensive law for cyber-protection in Israel is currently only in the drafting stage. This fact hinders government bodies from enforcing consistent cybersecurity standards and guidelines in the healthcare sector [21].

Regulation also can serve as a driving force, provided that the specific regulations are realistic and supported by adequate funding and enforcement. However, effective regulation must avoid the potential pitfalls indicated by the participants of this study of erring toward being overly vague or overly specific. In either case, the outcome is identical, as a regulation can be ineffective either by failing to define clear mandatory requirements or by being so specific that its requirements are impossible, leading, de facto, to the regulation being ignored. To avoid such pitfalls, we recommend that regulators avoid specifying particular technological solutions, which are likely to soon become obsolete, and instead follow the example of the European General Data Protection Regulation (GDPR) in setting ethical standards, as has been customary in the European Union since 2016 [30], together with legal repercussions and enforcement mechanisms.

3. Collaboration between Vendors and Health Professionals in Market Research and Product Development

Study participants indicated that they were not convinced that innovative cryptography-based data security systems would provide them with a significant ROI. It is unlikely that advanced technological approaches to securing patient data will be adopted unless key stakeholders in the health system understand the benefits and value of these techniques. Furthermore, these stakeholders need to be persuaded that these techniques offer significant benefits compared with current data management procedures. The study results showed that advanced security is not a high priority among individuals in key cybersecurity positions, who prefer systems that can also guarantee the business interests of the organization. In this regard, technology developers should consider collaboration with health professionals in market research and product development to ensure that new cyber-technologies offer high protection from cyber-attacks, together with accounting for the demand for efficiency and access to data within the healthcare sector.

In conclusion, health organizations face a growing threat of cyber-attacks on healthcare providers and their systems. Thus, it is essential to map the various stakeholders that manage and protect patient data in order to understand their different perspectives. The study findings point to several major barriers to the adoption of advanced cryptographic techniques within these organizations. These barriers are related to organizational priorities, work processes, and the limited resources available within healthcare organizations. We highlight ways in which cross-sectoral collaboration may help address these barriers to enhance patient data security and how these would benefit the healthcare sector and the public.

The findings of this study also suggest that one of the key factors that may account for reluctance to adopt cybersecurity technology is a lack of coordination between relevant stakeholders. For example, regulators craft policies and technical guidelines related to cybersecurity that health organizations may be unable to implement in practice. From another perspective, vendors that develop cybersecurity solutions for the healthcare setting sometimes fail to convince healthcare organizations that their products can offer added value over existing solutions and will be a worthwhile investment of limited organizational resources. These circumstances create obstacles to the coordination and standardization of cybersecurity technology and its implementation in healthcare at the national level. The study results support the call for stakeholders in the healthcare sector to work collaboratively to facilitate discourse related to constraints, opportunities, and stakeholder needs for the protection of patient data.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgments

The authors would like to thank everyone who participated in the interviews, and all the organizations that hosted us. The study was fully supported by The Center for Cyber Law & Policy (CCLP) in conjunction with the Israel National Cyber Directorate and the University of Haifa.

ORCID

Nehama Lewis (https://orcid.org/0000-0002-2130-2441)
Yaron Connelly (https://orcid.org/0000-0002-7924-9663)
Gil Henkin (https://orcid.org/0000-0003-3319-1045)
Max Leibovich (https://orcid.org/0000-0001-7027-3176)
Adi Akavia (https://orcid.org/0000-0003-0853-3576)

References

1. Miller DP Jr, Latulipe C, Melius KA, Quandt SA, Arcury TA. Primary care providers' views of patient portals: interview study of perceived benefits and consequences. J Med Internet Res 2016;18(1):e8.
2. Nausheen F, Begum SH. Healthcare IoT: benefits, vulnerabilities and solutions. Proceedings of 2018 2nd International Conference on Inventive Systems and Control (ICISC); 2017 Jan 19-20; Coimbatore, India. p. 517-22.
3. Kassam A. Spain will register people who refuse Covid vaccine, says health minister [Internet]. London, UK: The Guardian; 2020 [cited at 2022 Mar 30]. Available from: https://www.theguardian.com/world/2020/dec/29/spain-to-keep-registry-of-people-who-refuse-covid-vaccine.
4. Akpan N. Has health care hacking become an epidemic? [Internet]. Arlington (VA): PBS NewsHour; 2016 [cited at 2022 Mar 30]. Available from: https://www.pbs.org/newshour/science/has-health-care-hacking-become-an-epidemic.
5. Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, et al. Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security 2021;105:102248.
6. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care 2021;33(1):mzaa117.
7. Ikeda S. Wave of cyber attacks hits US healthcare system as FBI warns of coordinated criminal campaign [Internet]. Singapore: CPO Magazine; 2020 [cited at 2022 Mar 30]. Available from: https://www.cpomagazine.com/cyber-security/wave-of-cyber-attacks-hits-us-health-care-system-as-fbi-warns-of-coordinated-criminal-campaign/.
8. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Secur 2020;18(3):228-31.
9. Evans D, Kolesnikov V, Rosulek M. A pragmatic introduction to secure multi-party computation. Found Trends Priv Secur 2018;2(2-3):70-246.
10. Gentry C. A fully homomorphic encryption scheme [dissertation]. Stanford (CA): Stanford University; 2009.
11. Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans Comput Theory 2014;6(3):1-36.

12. Fan J, Vercauteren F. Somewhat practical fully homomorphic encryption [Internet]. Bellevue (WA): Cryptology ePrint Archive; 2012 [cited at 2022 Mar 30]. Available from: https://eprint.iacr.org/2012/144.
13. Cheon JH, Kim A, Kim M, Song Y. Homomorphic encryption for arithmetic of approximate numbers. In: Takagi T, Peyrin T, editors. Advances in Cryptology – ASIACRYPT 2017. Cham, Switzerland: Springer; 2017. p. 409-37.
14. Alami H, Gagnon MP, Ahmed MA, Fortin JP. Digital health: cybersecurity is a value creation lever, not only a source of expenditure. Health Policy Technol 2019;8(4): 319-21.
15. Alqarni A. Exploring factors that affect adoption of computer security practices among college students [dissertation]. Ypsilanti (MI): Eastern Michigan University; 2017.
16. Ishikawa K, Ohmichi H, Umesato Y, Terasaki H, Tsukuma H, Iwata N, et al. The guideline of the personal health data structure to secure safety healthcare. The balance between use and protection to satisfy the patients' needs. Int J Med Inform 2007;76(5-6):412-8.
17. Siegek-Itzkovich J, Udasin S. Cyber attacks hit Israeli hospitals as globe battles new computer virus [Internet]. Jerusalem, Israel: The Jerusalem Post 2017 [cited at 2022 Mar 30]. Available from: https://www.jpost.com/israel-news/israel-thwarts-hackers-from-cyber-attack-on-hospitals-498256.
18. Shahaf T. Israel reports rare cyber attack on one of its hospitals [Internet]. Tel Aviv, Israel: Ynetnews; 2021 [cited at 2022 Mar 30]. Available from: https://www.ynetnews.com/business/article/bjc1ddesk.
19. Hillel Yaffe Medical Center. In record time: just one month after the cyberattack, Hillel Yaffe has returned to regular activity [Internet]. Hadera, Israel: Hillel Yaffe Medical Center; 2021 [cited at 2022 Mar 30]. Available from: https://hy.health.gov.il/eng/?CategoryID=23&ArticleID=1051.
20. The Israel Democracy Institute, Eli Horovitz Conference for Society and Economic. The health system's readiness for crisis scenarios [Internet]. Jerusalem, Israel: The Israel Democracy Institute; 2020 [cited at 2022 Mar 30]. Available from: https://www.idi.org.il/media/15311/health.pdf.
21. Weenk S. National Cybersecurity Strategies in the Healthcare Industry of Israel and the Netherlands: a comparative overview. Cyber Intell Secur 2020;4(1):107-29.
22. Jones CM, McCarthy RV, Halawi L, Mujtaba B. Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. Iss Inf Syst 2010;11(1):9-16.
23. Fishbein M, Ajzen I. Predicting and changing behavior: the reasoned action approach. New York (NY): Psychology Press; 2011.
24. Rogers RW. A protection motivation theory of fear appeals and attitude change1. J Psychol 1975;91(1):93-114.
25. Guba EG, Lincoln YS. Epistemological and methodological bases of naturalistic inquiry. ECTJ 1982;30(4):233-52.
26. Nowell LS, Norris JM, White DE, Moules NJ. Thematic analysis: striving to meet the trustworthiness criteria. Int J Qual Methods 2017;16(1):1609406917733847.
27. Harrell MC, Bradley MA. Data collection methods: semi-structured interviews and focus groups. Santa Monica (CA): Rand National Defense Research Institute; 2009.
28. Attride-Stirling J. Thematic networks: an analytic tool for qualitative research. Qual Res 2001;1(3):385-405.
29. Charmaz K. Constructing grounded theory: a practical guide through qualitative analysis. Thousand Oaks (CA): Sage Publications; 2006.
30. Voigt P, Von dem Bussche A. The EU general data protection regulation (GDPR): a practical guide. Cham, Switzerland: Springer; 2017.

Appendix 1. Protocol of the interview

<u>Opening:</u> Explain the research and attain informed consent.

1. Recent advances in the concrete complexity of advanced cryptographic tools, such as secure multi-party computation (MPC) and fully homomorphic encryption (FHE), have the potential to offer improved security for medical records by protecting not only data at rest or in transit but also data in use. This offers benefits of high security while supporting the desired data analytics functionality such as secure data retrieval and privacy preserving analytics and machine learning.

a. The perception and needs of the organizations in the healthcare system are valuable knowledge and that is why we turn to you – the experts – so that we can learn from you, what the needs are and how future systems can be adapted to the health system.

b. We strive to examine this at all levels and therefore we represent two fields of study: ___ (Interviewer 1) specializes in computer science and ___ (Interviewer 2) in health policy.

c. The study is completely anonymous. We wish to emphasize that you can ask that information provided here will not be used as data. We will ask your permission to fill out an informed consent document detailing the procedure of the interview and recording the interview and our request to record its course.

1. <u>Part One</u>: Understanding the current situation in the organization and technical details (Interviewer 1)

a. What kind of information do you store and secure?

i. What volume of medical records do you store?

ii. What types of processing and retrieval are done? At what rate?

iii. What is a typical rate and latency in data retrieval and processing in your organization?

iv. Where is the information physically stored? – Cloud? On-premise? Backups?

v. What are the information security methods used in the organization?

vi. Who is in charge of managing the information security aspect in your organization? – Local teams? Outsourcing? Combinations?

vii. Are there integrations with cloud-based external systems? how are they protected, is encryption used?

2. <u>Part Two</u>: Understanding the Organizational Culture (Interviewer 2)

a. On a scale of 1 to 10 – How do you describe the degree of threat of cyber hacking of patients' files / medical records, in your organization?

i. Who do you think will be at the highest risk, if and when such a breach occurs? – Patients? Doctors? Organizations? Others?

b. How do you think the organization is currently meeting the cyber challenges?

i. What are the advantages and disadvantages of your working methods?

c. Are the resources allocated to you today appropriate for the dangers?

i. What resources are you lacking?

ii. If you were to get an extra budget for only one or two purchases, how would you invest it?

iii. If you were to demand an extra budget for information security – would this be given? If not, why

3. <u>Part Three</u>: Discussion of advanced cryptographic methods for cybersecurity (Interviewer 1)

a. Have you heard of cryptographic methods for protecting data-in-use such as MPC and FHE? For example, Fully Homomorphic Encryption (FHE) allows computing any algorithm on encrypted input (ciphertexts), with no decryption or access to the secret key that would compromise secrecy, yet succeeding in returning the encryption of the desired outcome. Such a mechanism provides patient data protection but also allows utilization of it.

b. What do you **know** about it?

c. What do you **think** about it?

d. Are you currently using such methods in your organizations?

4. <u>Part Four</u>: Examining the feasibility of adoption (Interviewer 2)

a. If a system for protecting data-in-use was operational would you consider adopting it?

i. Could you elaborate why - yes/no?
ii. For participants who consider adopting such a system, ask:
1. What would the benefits of such a system be for your organization?
2. How much would you or your organization be willing to invest in it?
iii. For participants who will not consider adopting such a system, ask:
1. What are the disadvantages you perceive for introducing such a system into your organization?
2. Do you believe that adopting the technology is not feasible or problematic?
3. Is there an organizational or financial cost to consider?
4. Would the organization support you if you want to adopt?
5. Suppose the system is adopted by other organizations, would this incentivize adopting similar technology in your organization?

5. Part Five: Assessment of suitability (Interviewer 1)

a. To what extent does the method we have proposed conform to the standards of compartmentalization and security in the organization?

6. Part Six: Security Culture (Interviewer 2)

a. What is the main motivation to do a ‘good job’ in your department?
b. What are the added values for ‘excellent information security’ in your organization that go beyond data protection?
c. Who designs the organization’s information security policy in your organization? – You? Management? The healthcare system?

Conclusion: We thanked participants for participation. We emphasized the potential importance of the data collected in this study, provided assurances of confidentiality, and offered to share the research conclusions with participants.