Commentary on Healthcare and Disruptive Innovation

Hilary Finch[1,2], Affia Abasi-Amefon[3], Jung, Woosub[4], Lucas Potter[5] and Xavier-Lewis Palmer[1,2,5]

[1]Old Dominion University, Norfolk, USA
[2] CySecSol, Franklin, USA
[3] University of Tartu, Tartu, Estonia
[4]William & Mary, Williamsburg, USA
[5] BiosView, Oswego, USA

hfinc003@odu.edu
amefon.affia@ut.ee
wjung01@wm.edu
lpott005@odu.edu
xpalm001@odu.edu

Abstract: Exploits of technology have been an issue in healthcare for many years. Many hospital systems have a problem with "disruptive innovation" when introducing new technology. Disruptive innovation is "an innovation that creates a new market by applying a different set of values, which ultimately overtakes an existing market" (Sensmeier, 2012). Modern healthcare systems are historically slow to accept new technological advancements . This may be because patient-based, provider-based, or industry-wide decisions are tough to implement, giving way to dire consequences. One potential consequence is that healthcare providers may not be able to provide the best possible care to patients. For example, if a healthcare provider does not adopt new technologies or approaches to medical treatment, they may not be able to offer the same level of care as a provider who has embraced those innovations. This leads to lower quality of care and poorer patient outcomes. Another consequence is that healthcare providers who do not adapt to disruptive innovations may lose market share to competitors who are more forward-thinking and willing to embrace new technologies and approaches. This can harm the provider's financial performance and sustainability.Not adapting to disruptive innovations in healthcare can result in missed opportunities to improve the efficiency and effectiveness of medical treatment. If a healthcare provider does not adopt electronic medical records, they may miss out on the benefits of faster and more accurate information sharing, improving patient care. Once the decision to implement technology in a specific healthcare industry is made, concerns about patient safety, an aversion to change, and hospital-wide compliance with regulations begin to arise (WynHouse, nd.). The healthcare technology industry also boomed with the COVID-19 outbreak. The COVID-19 outbreak has led to significant advancements and innovations in medical technology. In order to diagnose, treat, and prevent the spread of the virus, healthcare providers and researchers have had to develop and deploy new technologies and approaches. The COVID-19 outbreak has highlighted the importance of the medical industry and the essential role it plays in society. This has led to increased funding, support for medical research and development, as well as a greater appreciation for the work of healthcare providers. This has created opportunities for growth and innovation in the medical industry. It also placed enormous strain on global health systems, disrupting healthcare by increasing the risk of fraud and deception; the risk of hospital operations and assets being compromised, disrupted, or altered; and the increased use of telehealth resulting in a breakdown between providers and consumers (Kuehn,2021). This article will cover the effects/impact of disruptive innovations/technologies introduced into healthcare industries over the short term through a light review of disruptions and responses, followed by commentary and policy recommendations.

Keywords: Healthcare, Disruption, Cybersecurity, Cyberbiosecurity, Biocybersecurity, Disruptive Innovation,

1. Background

For many years, the misuse of technology has plagued the healthcare system. "Disruptive innovation" offers an issue for healthcare systems, particularly in introducing new technologies. Historically, healthcare systems have developed or gained essential technology advances slower than other industries. The sluggish pace may be due to the difficulty of implementing patient-based, provider-based, or industry-wide technological decisions (Thimbleby,2013). Medical technology has the potential to significantly improve patient outcomes, but also carries risks. By taking a more cautious approach to introducing new technologies, healthcare providers can ensure that any new innovations are thoroughly tested and proven to be safe before they are widely adopted. Not all patients have equal access to healthcare, and the rapid introduction of new technologies can exacerbate existing disparities. By taking a more deliberate approach to introducing new technologies, healthcare providers can ensure that all patients have access to the care they need. The healthcare system is a complex and interconnected system, and the introduction of new technologies can have unintended consequences. By slowing the pace of technological change, healthcare providers can consider the long-term impacts of new innovations and ensure that they are sustainable over the long term. Further, if stakeholders decide to deploy technology in particular healthcare businesses, questions regarding patient safety, resistance

to change, and hospital-wide regulatory compliance arise (WynHouse, nd.). Although the medical instruments, drugs, procedures, and systems developed to improve people's health and quality of life are now simpler to use due to recent advancements in medical technology, their application across multiple departments remains challenged. The impact of this problem blunts the possibility of hospitals exploiting the near full potential of their technology, let alone their security technology. This brings into question if there is a disruptive innovation to be had at all.

The phrase "disruptive innovations" (DI) is new to the healthcare field. Because we now live in a digital age, healthcare should adapt its approach to technology, which should involve modifying how medical treatment is provided. If we do not adapt to healthcare technology, it could result in a lack of equitable access to medical care. This is because technology can play a crucial role in improving the accessibility of healthcare, particularly in underserved and remote communities. For example, the use of telemedicine and remote monitoring systems can allow healthcare providers to reach patients who may not otherwise have access to medical care.

Failing to adapt to healthcare technology can also result in preventable illnesses spreading to larger populations. This is because technology can help identify and track outbreaks of infectious diseases, and facilitate the rapid sharing of information and resources to contain and control the spread of these diseases. Not using technology to its full potential, we may miss out on opportunities to identify and address potential public health threats before they become widespread. Overall, the use of technology in healthcare can help to improve access to care and prevent the spread of preventable illnesses.

The disruption caused by DI leads to tremendous change, causing a ripple effect on how things are done across the business. Healthcare-specific disruptive innovations are not limited to devices or digital technologies but also cover innovations in basic science, diagnostics (i.e., pathological or radiological diagnostic discoveries), education, processes (i.e., novel health policies, new processes or roles like the introduction of nurse practitioners or patient assistants), and in technique (i.e., the introduction of novel medical techniques within a specialty) (Sounderajah et al.,2021). However, we focus our analysis on devices and digital technologies to explore the security ramifications of introducing these technologies into the healthcare industry.

1.1 Healthcare DI, types of healthcare DI, the scope of work

Popular examples of technological disruptions in the healthcare industry cover software applications, (i.e., mHealth applications, telehealth, patient data systems, and clinical decision support systems), devices, wearables, monitors, imaging, system infrastructure innovations through cloud computing, IoT, and blockchain, and other applied innovations using RFID , AR/VR, and AI The software applications such as the CDSS examine data contained within electronic health records to provide clinicians and other healthcare professionals with reminders and prompts to assist patients in receiving evidence-based guidelines, ultimately leading to improved care and records. (CDC, 2022). With applied innovations, AV/VR has been used to promote patient rehabilitation (Brooks,2014), while RFID makes it simpler for providers to track, communicate, and identify resources and patients (Haddara & Staaby, 2018). Recent developments in the healthcare industry have also brought on the necessity to implement AI in the healthcare context. AI can reduce healthcare costs by reducing staff burnout, reducing patient wait times, and tackling disease complexity(Bellucci,2002). These entail innovations in the form of using AI assistants to grade and sort patient images and text data, being able to address or at least route patient concerns through natural language processing modalities, to examine literature, patient data, and health care provider inputs to either decipher patient pathologies or solution(s) to patient pathologies and reduce harms and lawsuits that would result, among other innovations (Wynants et al., 2020; Shaheen,2021). Reflecting on benefits of these disruptive innovations and the move towards adoption, it is essential to consider the security implications of these proposed innovations, post-adoption, especially with the impact of COVID-19 on the industry.

According to Sounderajah et al. (2021), the concept of "disruptive innovation" has made its way into health care. The article discusses the outcome of a systematic review, characterizing and categorizing the concept of “disruptive innovation” into basic science, device, diagnostics, digital health, education, processes, and technique. The paper also discussed great interest in technology-related innovations such as "omics” technologies, mobile health applications, telemedicine, and health informatics. However, the authors highlight that the use of disruptive innovation remains inconsistent, and its current definition does not accommodate exploration, especially for policymakers.

1.2 Related Work with process considerations in Healthcare DI

The main aim of this study is a commentary and light examination of the notion of "disruptive innovation" in healthcare within the scope of cybersecurity. Sensmeier claims that healthcare employees see the growth of technological innovation in their daily lives (Sensmier,2012). The use of smart patient care equipment, electronic patient care files, blood glucose meters, and portable gadgets in healthcare disruption can be a vital tool for constructing a higher quality, more convenient, and lower cost healthcare system. In this study, Sensmeier claims that advances in healthcare technology will allow people to experience faster, more individualized care (Sensmier, 2012).While technology is improving and new ideas are being introduced, the healthcare system is becoming more complicated, inefficient, and stressful for practitioners (Harris,2018). This article supports the idea that every organization's culture should encourage strong technical communication and coordination among clinicians worldwide. Still, the infrastructure needs to be able to support new ideas that improve workflow and make it easy to use relevant technical or institutional knowledge at the point of care. By leveraging disruptive innovation, incorporating evidence into care delivery and decision-making, involving patients and families in healthcare decisions, and improving care coordination across organizations, we will accelerate progress toward improving our nation's health.

Yellowlees et al. (2011) state that asynchronous medicine would thrive within a facilitated network model, which would change the jobs of most of the people involved in caring for a patient. The facilitated network model would consist of an electronic system through which healthcare professionals and patients share information, like transmitting healthcare records. This practice is formally known as "precision medicine." Precision medicine includes the delivery of patient-specific, focused treatment. This is accomplished by utilizing electronic health records (EHRs) to enhance patient outcomes.Yellowlees et al. (2011) asserts that while asynchronous medicine may be well-established and advantageous in specialties like radiology, there is little research regarding the benefits of asynchronous medicine in areas that traditionally rely on physical doctor-patient interaction. A transition to asynchronous medicine would significantly change the roles of primary care doctors, specialists, patients, and nonmedical providers. It states that putting asynchronous data sets into patient records would make it easier to compare patients over time and between groups and make it possible to get second opinions without requiring excessive and unnecessary travel from the patient. While this may make healthcare optimal, we could open ourselves up to future vulnerabilities. It is reportedly common for radiologists to work remotely (Yellowees et al, 2011). Patient data is sent to these outside of network workstations. However, after reviewing previous work evaluating disruptive innovation in healthcare, we find that cybersecurity aspects of these innovations in their development and adoption by the healthcare industry remain under-examined. Due to the benefits of disruptive innovations, we must raise cybersecurity concerns that harm healthcare services and patients.

2. Healthcare DI pre-pandemic, security considerations

Before the pandemic, there were already many specialized hospital information systems, like electronic health record (EHR) systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems, and computerized physician order entry systems. These information systems, widely used by many hospitals and other healthcare facilities, are highly specialized and collect, manipulate, process, store, and depend on patients' personal and sensitive information. There are several different types of EHR systems that are utilized in the healthcare setting, and they have their own particulars in security needs (Adracare, nd.). As the healthcare sector has more potential for harm than nearly any other industry, cybersecurity should be a priority alongside DI, but it is not (Schulman et al,2009). Alarmingly, Jalali and Kaiser (2018) noted that "70% of hospital boards include cybersecurity in their risk management oversight, and only 37% of hospitals perform annual incident response exercises." Just in 2021, there have been 108 individualized ransomware attacks that affected 2,302 medical facilities. Within these facilities, it was estimated that 19.76 million patient records were impacted. Thes attacks cost the medical facilities $7.8 billion in downtime (Bischoff,2021). These indicate major gaps in hospital security oversight and help explain numerous hospital attacks. Hospital organizational culture had insufficient threat and vulnerability awareness or preparation. Further, they cannot guarantee the availability of resources for the product they promote or use. This problem has been long-running. Garret et al. (2006) found in the analysis of rural hospitals that the drive to use technology to address US healthcare problems was hampered through sub-optimal utilization; at the time, less than 10% of hospitals had an electronic medical record with an estimated less than 20% of healthcare providers utilizing complete computerized patient records. This has improved, according to Healthit.gov, which stated, "In data from 2019 and 2021, 86% of non-Federal general acute care hospitals had adopted a 2015 Edition certified

electronic health record (EHR). In contrast, only 40% of rehabilitation hospitals and 23% of specialty hospitals had adopted a 2015 Edition certified EHR," (*Adoption of electronic health records by hospital service type,2019-2021*). Nonetheless, hospitals have far to go in optimally using electronic records.

3. Barriers associated with data-sharing with DI technologies

DI technology definitionally requires adjustment. Lack of policy, norms, or quality may be technical. To meet the healthcare industry's changing needs, software, installation, upgrades, and equipment optimization cost money. (AAP, nd). The presence of a competitive market, networks, and systems that make it easy to exchange data and personally identifiable information at risk can all act as trust obstacles. This might be because of the reliance on vendors and market providers, who have relaxed regulations regarding data protection, causing a person authorized to access protected health information at a covered entity to disclose the information inadvertently due to a breach of security at the covered entity (HIMSS, nd).

4. Malware of Various Types, Including Ransomware

There are a variety of additional forms of malware, like ransomware, that pose a threat to healthcare providers and organizations. Examples include ransomware, Trojans, and phishing. Phishing is particularly effective since it is directed at the specific user and attempts to dupe the user into giving sensitive information, clicking on a malicious link, or opening an infected file using social engineering techniques. Emails sent using spear phishing to target specific individuals have a higher success rate than emails sent using broader tactics. When it comes to cybersecurity in the healthcare industry, a comprehensive incident response strategy is required to ensure that potential security breaches are prevented or dealt with promptly and effectively. This is to protect the patient's personal information. For instance, an assault was launched against the information technology department at the University of Vermont Medical Center as recently as October 2020. During the nearly one month without EHR (electronic health records) and other essential medical technology, the staff at UVMC worked using paper tools. The resolution of this assault took over a month, and even though the company chose not to pay the ransom but instead to shut down its networks, the estimated cost of the attack was still around fifty million dollars (AAMC, nd).

These factors might cause providers to struggle, including the cost to the business, the time spent learning new software, the legality of the software and its data collection and restrictions, the fear of learning new ways of doing things, the usefulness of the product, and the complexity of implementing the new DI technology. Interactions between the device and the user are referred to as "human factors" in medical device equipment. Everything from the device's size, shape, and controls to how intuitive it is to use and how well the instructions are written contributes to the device's usability. Human factors in medical device design focuses on making sure the device isn't dangerous to the user and can be operated with minimal effort and time loss.

DI software and technology are not designed with the provider in mind. Some of this results in real or perceived increased effort for personnel. Rural medical facilities should be taken into account because they have unique problems with adopting DI because they don't have enough staff, space, or reliable internet access. According to a 2018 FCC estimate, 31% of rural households in the United States still do not have access to broadband internet (Eighth Broadband Progress Report, nd). Some DI decisions also disrupt patient life owing to the complexity of the program and its applications, a lack of access to information or insufficient information available to the patient, or the technology itself being limited in its use. Cultural issues for digital services include telehealth, telemonitoring, technological skepticism, digital literacy, the expense of required hardware to operate the program, and device compatibility. To take a page from Garrett et al. (2006), patients must understand the privacy and security policies involved in their care, along with how to keep their information private and secure.

5. Healthcare DI during and post-pandemic, security considerations

Covid-19's healthcare technology expansion boom placed enormous pressure on health systems globally, disrupting healthcare services by raising the risk of fraud and deception, altering and interrupting cyberbiosecurity, and creating a breakdown between providers and consumers through the increased use of telehealth (Kuehn, 2021). The pandemic gave perfect conditions for a spike in ransomware attacks on healthcare institutions like the Brno University Hospital in the Czech Republic, the World Health Organization, and other healthcare supply chains (He et al., 2021). Ransomware attacks within an industry would increase in frequency and pay, making the healthcare system even more fragile than before the pandemic.And as healthcare companies improve their cybersecurity defenses, criminals adopt new modus operandi to maximize financial

gain by executing more complex attacks within a single breach, often leading to a complete system shutdown (Lang et al.,2021). Tracking systems, technology-based social distancing, mobile app-based contact tracing systems, telemedicine consultations, e-quarantine technology, AI-based patient care, QR code check-in systems, and AI-based temperature scanning are all examples of innovations in the healthcare sector that resulted from the impact of COVID-19 (Liu et al.,2022). Various interviews with hospital professionals and managers revealed that, subsequently of the COVID-19 epidemic, digital care has increased (Lee et al.,2021). The pandemic encouraged the need for hybrid healthcare services to deliver continuous enhanced service thanks to the innovation of digital technology (Liu et al. 2022). The COVID-19 pandemic was also a large factor in facilitating the growth of digital health technology (DHT). DHT is the fusion of digital technologies with society, health, and medical care. With the prioritization of DHT to “flatten the curve," DHT innovations are at the forefront of DI technology (Whitelaw et al., 2021). These innovations are changing how we treat and deliver patient care. As discussed in the previous sections, medical technology was already slow to implement, and the pandemic brought the same doubts and fears, widening the gap between technology and providers.

6. In the scope of COVID-19 and cyberbiosecurity

Many people are concerned with the amount of information and data that must be sacrificed to receive quality care. While these were concerns before the pandemic, the onset of COVID-19 increased the necessity of securing digital resources due to the increased threat of cyber-attacks by threat actors (Adler et al.,2021).

Contact-tracing Privacy is about tracking and identifying people who have had contact with a person or people who are sick. This method of identifying and monitoring individuals who may or may not be sick has been around for centuries (Contact Tracing, nd). In past years, contact tracing was a manual process that was limited in identification and notification within a quality time frame to cause the least harm. Notably, the past infectious diseases that were traced were for infections of less than 10,000 people worldwide, whereas COVID-19 has infected 619 million as of this writing (WHO,2022), proving the need for other options for contact tracing. The use of cell phones for contact tracing began innocently enough; it was a quick, efficient, and discretionary way to spread COVID-19 infection information. In the age of technology, most people’s personal information is stored on their devices: banking services, biometrics, credentials, and access to healthcare portals with known vulnerabilities. By allowing countries to use or access location services of smart devices in an attempt to contact trace, the end user is opening themselves to security threats and vulnerabilities leading to unauthorized access to personally identifiable information. An alternative method of contact tracing with more privacy is the use of Bluetooth technology in place of location services. Bluetooth collects significantly less information; some of it is voluntary, like phone numbers. This technology detects if you have been close to an infected person(s) and notifies you only if you have been in the same area as the infected individual without invading the infected individual's privacy, which is useful for the general public. It hinders the contact tracing process, as the entire connection and divulging of PII is completely voluntary, leaving it open to human error and false reporting. The COVID-19 pandemic showed how important it is to keep track of disease data for researchers, policymakers, and the general public. The disease data includes the number of cases, the results of diagnostic tests, and information about general trends, which makes it a target for malicious actors.Diagnostic testing and counting are highly valuable and used to measure epidemic levels, making it potentially catastrophic if the surveillance data is compromised (Adler et al.,2021).

7. Policy recommendations and solutions to security challenges with Healthcare DI (pre during-post pandemic)

Taking focused facilities and user networks out of the current mixed healthcare delivery models could save money and be more efficient. Still, it could also break up the way care is given. Care coordination can also be done differently by a patient-centered medical home, telephonic services, web-based decision-making software, and personal health records. But it is important to remember that the healthcare system comprises many business models that depend on each other. Policymakers in health care need to be aware of the hidden cost of supporting and renewing rules that slow down innovation in the long run. With less money, hospitals and doctors have to work even harder to meet their value proposition of providing complex and expensive medical care. They are even less likely to give work to businesses that add value (Hwang et al.,2008). The topic of cyberbiosecurity is very multidisciplinary, and it will be beneficial to integrate the skills and methodologies already in use from various sectors with the requirements posed by the life sciences. Several other cyber applications have been proposed as potential solutions to some emerging problems regarding cyberbiosecurity. Putting them into reality might be difficult because even the most fundamental concepts of information security

require improved adaptation to the framework of bioscience. Similarly, it will be necessary to hone and expand the traditional CIA triad (confidentiality, integrity, and availability) and extend the ideas made earlier to match them properly with the current requirements. Traditional cybersecurity concerns are not always relevant to all of the newly discovered difficulties. Therefore, it will be essential to figure out which difficulties the currently available cyber-approaches could or could not discover or guard against. There is a need for a rethinking of quality assurance testing since the completed product or system may not appear exactly like what was stated (in digital form). Quality control and assurance measurements only show how a biological system was and is. They cannot predict the future or provide enough information for cyber defense. Safeguarding policies should consider the unique qualities of "information" in the biological sciences, the life cycle of information in its broadest sense, logically-based game strategies, mechanisms for dual-use appropriation, end-to-end assessments, "routes to harm" in context, and multiple exposure pathways (Mueller,2021). It has been demonstrated that some DI technologies can lead to a redesign of the existing healthcare infrastructure. This might result in significant cost savings and make healthcare systems more sustainable. These DI technologies result in more person-centered healthcare by encouraging patients to become more active in their self-care, lowering the number of doctor's office and hospital visits, and the necessity for more extensive medical intervention. Medical devices and lifestyle/general-purpose apps will not be required to comply with the stricter definition, notified bodies, or clinical safety evidence. The stricter definition will not apply to lifestyle or general-purpose apps (Sheppard,2020). Laws and regulations can minimize complexity and uncertainty because they improve the predictability of the new technology. Despite the possibility of utilizing DI healthcare for its contribution to the healthcare architecture, the many regulatory processes intended to enhance patient confidence may be an obstacle to the success of this technology. There must be a balance between enabling patient trust and encouraging innovation (Sounderajah et al.,2021).

8. Discussion of results and future of DI in Healthcare

There exists noticeable uncertainty around using the phrase "disruptive innovation," even though it has become increasingly common in the healthcare business. Inaccurate identification might result in a lack of understanding regarding the characteristics and potential of an innovation. This can lead to a delay in translating its benefits into actual economic and health outcomes because we do not understand the probable barriers to adoption and how to overcome them. Finding examples of truly disruptive technologies in the health sector is hard. While there are suggestions to classify upgraded technology as DI, none of these technologies have been able to change the market in a big way. None have changed healthcare significantly or led to the creation of new and better ways to deliver healthcare. Using AI as an example, several innovations are complicated, providing the opposite of an expected disruption. Panch et al. (2019) found several hiccups in the quest for AI to usher positively in disruptive innovation. It was noted in the vein of predictive medicine through Hermansson and Kahan (2018) that overtraining an AI healthcare algorithm on Caucasian data produced poorer predictive care for non-Caucasian groups. This issue falls in line with the poor application of AI in other areas and is an example of how their use has far to go in suitability for routine, un-aided use without perpetuating negative or unhelpful feedback loops of care (Costanza-Chock et al. 2022; Hoffman,2021; Gebru,2020; Kong,2022). Many sources of electronic medical records systems hold incomplete connectedness, communication, and completeness, making it difficult for them to be used optimally (Patch et al.,2019). This could compound the quality of assistance being lent by AI assistants. With all applications of AI, and “innovations” in general, it can be their auditing, internally and externally, is important, especially when their impact remains new and poorly understood. Constanza-Chock et al., (2022) note a need for greater attention to AI audits performed by AI operators to reduce harm to stakeholders. Further, governments must be aware of and respond adequately to AI implementation in healthcare. The healthcare industry cannot function without contact between government and business through laws, professional standards, and administrative procedures. We need to be on the same page for significant disruption, and we are not there yet.

9. Concluding Remarks

Here,we provide a review and an analysis of a case study on the use of technology in healthcare services. We analyzed the approaches taken by the healthcare industry before the pandemic, during, and post-pandemic to recognize any impediment to genuine disruptive innovation. Major security lessons learned can be condensed in the understanding that efforts in implementing cybersecurity in hospital medical contexts are scattered throughout sites, are hampered by inefficiencies in organizational cultural absorption, and remain ultimately slow enough to be ahead of malicious actors. This relegates institutions to remaining reactive. This phenomenon

aligns with Sounderajah et al. (2021) that there has been little evident "disruptive innovation," only technological advancements. For "disruptive innovation" to exist, it must be accessible to everyone who is expected to utilize it. Further, there needs to be wider organizational and cultural technological literacy and agility to suitably adapt the components of such innovation. The aforementioned medical devices may become DI technology when extensive availability of the technology and ubiquitous base policy, legislation, and usage is the norm. Otherwise, we risk furthering hubris and wasting further resources on technical roads to nowhere.

Acknowledgements:

The authors would like to thank Jesse Finch for his contributions to editing.

References

Adler, A., Beal, J., Lancaster, M., Wyschogrod, D. (2021). Cyberbiosecurity and Public Health in the Age of COVID-19. In: Trump, B.D., Florin, MV., Perkins, E., Linkov, I. (eds) Emerging Threats of Synthetic Biology and Biotechnology. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-2086-9_7

Agency outlines barriers, progress in adoption of nationwide electronic health information system | AAP News | American Academy of Pediatrics. (n.d.). Accessed October 18, 2022,https://publications.aap.org/aapnews/news/7392?autologincheck=redirected?nfToken=00000000-0000-0000-0000-000000000000

Anita Ramsetty, Cristin Adams, Impact of the digital divide in the age of COVID-19, Journal of the American Medical Informatics Association, Volume 27, Issue 7, July 2020, Pages 1147–1148, https://doi.org/10.1093/jamia/ocaa078

Bellucci, N. (2022). Disruptive Innovation and Technological Influences on Healthcare. *Journal of Radiology Nursing*.

Brooks, Anthony Lewis. "Disruptive innovation in healthcare and rehabilitation." In *Technologies of Inclusive Well-Being*, pp. 323-351. Springer, Berlin, Heidelberg, 2014.

Contact tracing: how physicians used it 500 years ago to control the bubonic plague. (n.d.). Accessed October 18, 2022https://theconversation.com/contact-tracing-how-physicians-used-it-500-years-ago-to-control-the-bubonic-plague-139248

Costanza-Chock, S., Raji, I. D., & Buolamwini, J. (2022, June). Who Audits the Auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1571-1583).

Cybersecurity in Healthcare | HIMSS. (n.d.). Accessed October 18, 2022https://www.himss.org/resources/cybersecurity-healthcare

Eighth Broadband Progress Report | Federal Communications Commission. (n.d.). Accessed December 8, 2022, from https://www.fcc.gov/reports-research/reports/broadband-progress-reports/eighth-broadband-progress-report

Garrett, P., Brown, C. A., Hart-Hester, S., Hamadain, E., Dixon, C., Pierce, W., & Rudman, W. J. (2006). Identifying barriers to the adoption of new technology in rural hospitals: a case report. Perspectives in health information management, 3, 9.

Gebru, T. (2020). Race and gender. *The Oxford handbook of ethics of AI*, 251-269.

Haddara, M., & Staaby, A. (2018). RFID applications and adoptions in healthcare: a review on patient safety. *Procedia computer science*, *138*, 80-88.

Harris, D. A., Haskell, J., Cooper, E., Crouse, N., & Gardner, R. (2018). Estimating the association between burnout and electronic health record-related stress among advanced practice registered nurses. Applied Nursing Research, 43, 36-41.

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 23(4). https://doi.org/10.2196/21747

Hermansson, J., & Kahan, T. (2018). Systematic review of validity assessments of Framingham risk score results in health economic modelling of lipid-modifying therapies in Europe. *Pharmacoeconomics*, *36*(2), 205-213.

Hoffmann, A. L. (2021). Terms of inclusion: Data, discourse, violence. *New Media & Society*, *23*(12), 3539-3556.

Hwang, J., & Christensen, C. M. (2008). Disruptive innovation in health care delivery: a framework for business-model innovation. Health affairs, 27(5), 1329-1335.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research, 20(5), e10059.

Kilsdonk, E., Peute, L. W., & Jaspers, M. W. M. (2022). Factors influencing implementation success of guideline-based clinical decision support systems: A systematic review and gaps analysis. International Journal of Medical Informatics, 98, 56–64. https://doi.org/10.1016/j.ijmedinf.2016.12.001

Kuehn, B. M. (2021). Despite Improvements, COVID-19's Health Care Disruptions Persist. JAMA, 325(23), 2335–2335. https://doi.org/10.1001/JAMA.2021.9134

Kong, Y. (2022, June). Are "Intersectionally Fair" AI Algorithms Really Fair to Women of Color? A Philosophical Analysis. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 485-494).

Lang, M., Connolly, L. Y., Taylor, P., & Corner, P. J. (2021). The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks. Digital Threats: Research and Practice. https://doi.org/10.1145/3558006

Lee, S. M., & Lee, D. (2021). Opportunities and challenges for contactless healthcare services in the post-COVID-19 Era. Technological Forecasting and Social Change, 167, 120712.

Liu, Z., Shi, Y., & Yang, B. (2022). Open Innovation in Times of Crisis: An Overview of the Healthcare Sector in Response to the COVID-19 Pandemic. Journal of Open Innovation: Technology, Market, and Complexity, 8(1), 21.

Maria K Sheppard, mHealth Apps: Disruptive Innovation, Regulation, and Trust—A Need for Balance, Medical Law Review, Volume 28, Issue 3, Summer 2020, Pages 549–572, https://doi.org/10.1093/medlaw/fwaa019

Moran, M. (2016). Barriers to Adopting HIT Still Substantial, APA Tells Health Subcommittee. Psychiatric News, 51(20), 1–1. https://doi.org/10.1176/APPI.PN.2016.10B10

Mueller S. Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?. Biosaf Health. 2021;3(1):11-21. doi:10.1016/j.bsheal.2020.09.007

Adoption of electronic health records by hospital service type 2019-2021 (no date) HealthIT.gov. Available at: https://www.healthit.gov/data/quickstats/adoption-electronic-health-records-hospital-service-type-2019-2021 (Accessed: October 20, 2022).

Schulman, K., Vidal, A. & Ackerly, D. Personalized medicine and disruptive innovation: Implications for technology assessment. Genet Med 11, 577–581 (2009).https://doi.org/10.1097/GIM.0b013e3181ae0935

Sensmeier, Joyce E. MS, RN-BC, CPHIMS, FHIMSS, FAAN. Disruptive innovation and the changing face of healthcare. Nursing Management (Springhouse): November 2012 - Volume 43 - Issue 11 - p 13-14 doi: 10.1097/01.NUMA.0000421681.71712.86

Sera Whitelaw, Danielle M Pellegrini, Mamas A Mamas, Martin Cowie, Harriette G C Van Spall, Barriers and facilitators of the uptake of digital health technology in cardiovascular care: a systematic scoping review, European Heart Journal - Digital Health, Volume 2, Issue 1, March 2021, Pages 62–74,https://doi.org/10.1093/ehjdh/ztab005

Shaheen, M. Y. (2021). Applications of Artificial Intelligence (AI) in healthcare: A review. *ScienceOpen Preprints*.

Singh, S., Dhir, S., Das, V. M., & Sharma, A. (2020). Bibliometric overview of the Technological Forecasting and Social Change journal: Analysis from 1970 to 2018. Technological Forecasting and Social Change, 154, 119963.

Sounderajah V, Patel V, Varatharajan L, et al. Are disruptive innovations recognised in the healthcare literature? A systematic review. BMJ Innovations 2021;7:208-216.

The growing threat of ransomware attacks on hospitals | AAMC. (n.d.). Accessed September 20, 2022)https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

Thimbleby, H. (2013). Technology and the future of healthcare. Journal of public health research, 2(3), jphr-2013.

Types of Healthcare Information Systems - Adracare. (n.d.). Accessed December 15, 2022)https://adracare.com/2020/12/04/types-of-healthcare-information-systems/

WHO Coronavirus (COVID-19) Dashboard | WHO Coronavirus (COVID-19) Dashboard With Vaccination Data. (n.d.). Accessed October 18, 2022https://covid19.who.int/

Why is the Healthcare Industry Slow to Adopt Technology? - WynHouse Software. (n.d.). Accessed September 20, 2022)https://wynsoftware.com/wynmill/healthcare-slow-to-adopt-technology/

Wynants, L., Smits, L. J., & Van Calster, B. (2020). Demystifying AI in healthcare. bmj, 370.

Yellowlees, P., Odor, A., Patrice, K., Parish, M. B., Nafiz, N., Iosif, A. M., & Hilty, D. (2011). Disruptive innovation: the future of healthcare?. Telemedicine and e-Health, 17(3), 231-234.