https://doi.org/10.48009/1_iis_2020_118-124

Issues in Information Systems
Volume 21, Issue 1, pp. 118-124, 2020

CYBERSECURITY IN THE DENTAL HEALTHCARE SECTOR: THE NEED OF KNOWLEDGE FOR SMALL PRACTITIONERS

Eliel Melon, University of Puerto Rico, eliel.melon@upr.edu
Wilnelia Hernandez, Independent Researcher, wiheca@hotmail.com

ABSTRACT

Dental healthcare technology requires planning and time. This sector is a vulnerable organization to cyber-attacks and threats because they are not kept up with the threats. The objective of the study was to identify academic literature that present the problem of cybersecurity in dental healthcare and the necessity to expand the literature as an educational resource for these small medical practitioners. The researchers did a systematic literature review and conducted searches through four databases. Using keywords and database filters they found 4 articles that met the criteria. The analysis showed that this sector lacks knowledge in cybersecurity and there are not enough threats documented in the academic literature about these specific practitioners. The dental healthcare industry is a prime target right now, because of a phenomenon to digitalize all of the equipment during the past years. Time and economic resources must be invested to maintain and ensure the protection of dental healthcare technologies and the confidentiality of patient information from unapproved access. In our findings, this systematic literature review confirms the necessity to expand the amount of academic literature of cybersecurity for dental practitioners and consideration of creating a model solution that will help other small medical practitioners.

Keywords: cybersecurity, threats, dental healthcare, cyber-attack, resilience, cyber resilience, holistic, systematic literature review

INTRODUCTION

Healthcare technologies have the potential to extend, save and enhance lives (Coventry & Branley, 2018). Unfortunately, those technologies can introduce a potential cybersecurity risk if they are not properly maintained. Kruse, Frederick, Jacobson & Monticone (2017) stated that there are growing concerns that cybersecurity within healthcare is not sufficient and this has already resulted in a lack of medical information confidentiality and integrity of data. According to Cabaj et al. (2018), cybersecurity is considered an independent discipline. It is a "computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries" and involves the creation, operation, analysis, and testing of secure computer systems; and also includes aspects of law, policy, human factors, ethics, and risk management (Cabaj et al., 2018).

The problem of information security breaches in healthcare has been increasing every year. Statistics predictions show that cybersecurity breaches will continue in the arising. Hackers and cybercriminals know the high cost of a healthcare record and also know the existence of this problem and the fragile of the infrastructure. The government knows that these breaches exist, but there's no sufficient legislation to establish specific responsibilities to the people that manage the information of the patient. Some penalties exist, but it does not resolve the problem. In 2017 a task force was created, but today in 2020, cybersecurity breaches still impact the economy, the information of the patient, the government, and providers. In August 2019 a big cybersecurity threat was reported that affected dental offices (Coller, 2019). The threat was with ransomware that encrypted the information. As a small practitioner, economic resources are limited, but the threats are a reality. A universal electronic health (EHR) record appeared in the literature as a recommendation, but the reality in the practice is different (Hillestad, et al., 2005).

The first purpose of this systematic review is to identify specific cybersecurity literature for dental offices as small practitioners. The second purpose is to present the need to expand the amount of this specific type of literature for these practitioners. Studies affirm that education will help in the reduction of cyber threats. There is a large body of literature in the medical community, but for dental clinicians, there is not a large body of research addressing the topic of cybersecurity for equipment used by this community. We observe that every year, new technological equipment is created for this community and it is important for dental doctors to know how to protect them from any computer attack.

OVERVIEW

Dental Healthcare

Different professions have federal regulations to comply. Before a medical practitioner like a dentist can operate and offer their services, they need to comply with these regulations. This kind of practitioner needs to comply with HIPAA (Lisbon, 2018). Dental healthcare manages confidential patient information like the electronic record. An EHR (Electronic Health Record) does not guarantee the security of the information but provide the mechanism to protect the information. Like other small practitioner, dental offices need the implementation of cybersecurity tools to protect the privacy, integrity and confidentiality of the electronic protected health information (ePHI). Practitioners must understand the scope of the law compliance and the preparedness required. As a small office, dental practitioner's need to comply even if their cyber resources are limited (Health Care Industry Cybersecurity Task Force, 2017). A fundamental education and basic training are important during the university years (Scarbecz & DeSchepper, 2018). The knowledge of information security and the correct manage of the ePHI are neuralgic to understand the responsibility in law that they have as a healthcare practitioner.

HIPAA, HITECH, HITRUST

According to the Office for Civil Rights (OCR) (n.d.), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. The Health Information Trust Alliance (HITRUST) is a nonprofit organization that worked with the industry to create the Common Security Framework (CSF). To summarize the meaning of HIPAA, HITECH and HITRUST, the first one is the law, the second is a way to comply with the law and the third is an organization that helps to the compliance. According to HIPAA Journal - News and articles about HIPAA. (n.d.), the fine of a violation of HIPAA may vary. It can be:

- A violation of HIPAA attributable to ignorance can have a fine of $100 – $50,000.
- A violation that occurred despite reasonable vigilance can have a fine of $1,000 – $50,000.
- A violation due to willful neglect which is corrected within thirty days will have a fine between $10,000 and $50,000.
- A violation due to willful neglect which is not corrected within thirty days will have the maximum fine of $50,000.

Healthcare practitioners need to comply with the federal regulations. There are specific details according to the type of practitioner, but in general, the regulation to protect patient's information is required.

Social Media, SMS and Email

The new generation utilizes smartphones as part of their daily basis (Singh, Bhat, & Pawar, 2019). When manage ePHI the rules are different. HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework (2014), stated that "it mandates administrative, physical, and technical measures to safeguard the confidentiality, integrity, and availability of electronically protected health information (p. 2)". The instant messaging (IM) and email accelerate the answer of questions or consultant with colleagues, but in the medical office is necessary the use of the corresponding technology tools for this type of consult. According to Symantec (2019), small organizations have more vulnerabilities with email threats compare with large organizations. According to HIPAA Journal (2020), major instant messaging services are not encrypted and do not provide a recall option. If the practitioner uses this tool, the important detail is that they cannot share any ePHI in the messaging. Also, related to SMS, IM, and email, HIPAA Journal (2020) stated that "these safeguards require the introduction of access controls, audit controls, integrity controls, ID authentication, and transmission security to prevent unauthorized access to PHI". Literature affirms that the use of email can be affected by a phishing data breach problem (McLeod, & Dolezel, 2018). HIPAA Journal (2020) presented a case of a dental practitioner that uses Yelp® to respond to a patient comment and revealed confidential information. The practitioner had to pay a fine due to a violation of HIPAA regulation. Healthcare practitioners need to understand the regulations of the integration of new technologies, before they can be used in the office with ePHI. Social media is not a place to discuss any case of the patient (Plunkett, 2019).

Cyber Resilience

As a small practitioner, dental offices need resilience tools to minimize the impact of a cyber threat. The literature presents different kinds of basics steps to recover the office service in case of a ransomware or other data breach, but it is important to have a plan to be resilient in the case of a cybersecurity threat. According to Ortiz‐de‐Mandojana and Bansal (2016), the term resilience has two parts that include different actions by the organization, but in this paper, we just only want to present one of these. Ortiz-de-Mandojana and Bansal (2016) mentioned, that organizations have to manage unexpected situations. This is the part of the definition that we are going to cover. The Report on Improving Cybersecurity in the Health Care Industry (2017) stated that "poor cybersecurity practices at any level can become the cause of a breach and leave patients exposed to unexpected harm to their privacy or even the care they receive" (p. 44). Also, Sabillon, Cavaller & Cano (2016) stated that,

> The US Department of Homeland Security (DHS) conceived the Cyber Resilience Review (CRR) framework to assess cybersecurity capabilities thus cyber resilience within critical infrastructure and crucial resources sectors.
>
> The CRR is assembled in ten domains:
> 1. Asset management
> 2. Controls management
> 3. Configuration and Change management
> 4. Vulnerable management
> 5. Incident management
> 6. Service continuity management
> 7. Risk management
> 8. External dependency management
> 9. Training and awareness
> 10. Situational awareness (p. 76)

As a small practitioner, dental offices should include a simple routine to be cyber resilience in case of a cybersecurity threat. A recommendation can be, to follow the ten domains mentioned before and establish the corresponding plan of it. Also, it is recommended the integration of a certified EHR (Kalenderian, Walji & Ramoni, 2013). All employees must frequently change their passwords and use two-factor authentication (Mohammed, Mariani & Mohammed, 2015; Sabillon, Cavaller & Cano, 2016). Another recommendation is that practitioners need to integrate a plan of recurrent updates of all device's software, including operating systems (Lisbon, 2018) and frequently user training and awareness to review the practices and new trends (Sabillon, Cavaller & Cano, 2016). It is important the integration of information technology training (IT) (Hoffman, Burley & Toregas, 2011; Scarbecz & DeSchepper, 2018) with devices and information systems in the office. According to the Health Industry Cybersecurity Practices: Managing threats and protecting patients (2017), the establishment of a data backup, its corresponding test, and the secure process its recommended.

Holistic

Literature confirms the problem and initiative of cybersecurity across the world (Sabillon, Cavaller & Cano, 2016). As a medical office, dentists are integrating new technologies and information systems to manage patient treatment and patient information. The HIPAA Journal (News and articles about HIPAA, n.d.) shows the dramatic numbers of the impact of data breaches in healthcare systems. A holistic approach is emerging as an amplification of the panorama that HIPAA covers (Appari & Johnson, 2010; Hoffman, Burley & Toregas, 2011; Efe & Calik, 2018). It is not only the implementation of an EHR or ePHI. It is a complete vision of the details that are considered with the compliance.

Cybersecurity issues need a holistic view. Recently, the Report on Improving Cybersecurity in the Health Care Industry (2017), stated that "this will demand a systematic approach for understanding, modeling and reducing risk, and compromise at multiple points in the infrastructure used to deliver care"(p. 23). In a point of view, HITRUST will provide tools like a holistic approach as a non-profit organization to facilitate medical practitioner and healthcare providers comply with the federal regulations. Also, the tools, educational resources, and information that HIPAA Journal provides, help practitioners with the perspective of a holistic approach and with the accessibility to the information to modeling and reducing risk to facilitate the comply. As small practitioners, dental offices do not have the resources that hospitals or other big healthcare providers have, but the requirement to comply is the same and it is imperative that follow the checklist that is provided and view the comply with a holistic approach to optimize their resources (Lisbon, 2018; Sabillon, Cavaller, & Cano, 2016).

METHODS

The researchers derived the structure of this systematic literature review from the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) and the work of Kruse, Frederick, Jacobson & Monticone (2017). Articles were eligible for this review if they were published in the last 10 years if the full-text version of the manuscript is with PubMed, ProQuest, Google Scholar or Science Direct, and if the publication is a peer-reviewed and scholarly journal.

Four separate databases were queried to gather appropriate literature related to cybersecurity and dental healthcare. Databases chosen by the researchers included PubMed, ProQuest, Google Scholar and Science Direct. The search string used in all two research databases was “cybersecurity” AND “dental healthcare”. The literature search process is illustrated in Figure 1.

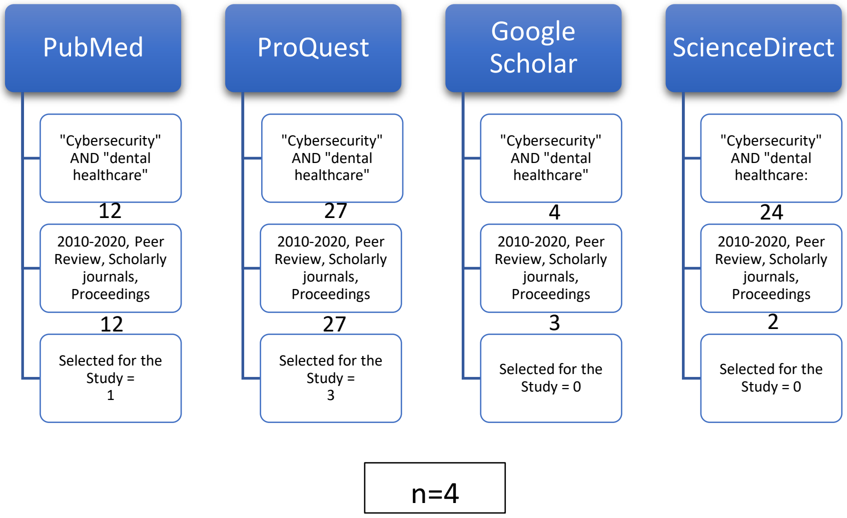
PubMed
"Cybersecurity" AND "dental healthcare"
12
2010-2020, Peer Review, Scholarly journals, Proceedings
12
Selected for the Study = 1
ProQuest
"Cybersecurity" AND "dental healthcare"
27
2010-2020, Peer Review, Scholarly journals, Proceedings
27
Selected for the Study = 3
Google Scholar
"Cybersecurity" AND "dental healthcare"
4
2010-2020, Peer Review, Scholarly journals, Proceedings
3
Selected for the Study = 0
ScienceDirect
"Cybersecurity" AND "dental healthcare:
24
2010-2020, Peer Review, Scholarly journals, Proceedings
2
Selected for the Study = 0
n=4

Figure 1. Literature Search Process

A common search string was used in all databases: (“cybersecurity” AND “dental healthcare”). The searches in all databases yielded very small results, even with filters. We used Peer Review and Scholarly journals as our filters. All literature included in the study was independently read by both researchers. Before the researchers accepted the literature, it was evaluated to ensure it was relevant to the study. Literature was only rejected and excluded if both researchers agreed it was not relevant.

A total of 4 articles were identified or related in the “cybersecurity” AND “dental healthcare” search. Most of the literature was in the form of articles in journals. It was a very small sample. The final sample size was 4.

RESULTS

The initial search produced a total of 44 articles relating to the search topics "cybersecurity" AND "dental healthcare". As we had said before, articles were eligible for this review if they were published in the last 10 years, if the full-text version of the manuscript it is in the databases, and if the publication is a peer-reviewed and scholarly journal. After the researchers filtered the search criteria, there were only 4 articles selected. One article was selected from the PubMed database and 3 articles were selected from the ProQuest database. Table 1 provides a list of all the articles relevant to the study in the systematic review as well as a brief synopsis of their content and the focus of it.

All of the articles analyzed are in agreement with the growing threat of cyber-attacks in healthcare. Some of them are specifically talking about the dental healthcare sector. The researchers found that there is a very small amount of studies that cover the topics of cybersecurity in dental healthcare. According to Loughlin, et al. (2014), many IT experts are concerned that recent trends will convince cybercriminals to target medical devices. It is important to develop more studies in this direction because new technologies are emerging in the dental sector and these practitioners will need to know about the best practices to deal with this type of cyber threat.

Table1. Articles Observations

Author(s)	Synopsis	Focus
Plunkett, L (2019)	New York State SHIELD (Stop Hacks and Improve Electronic Data Security) Act that Gov. Cuomo signed into law on July 25, 2019, as Chapter 117 of the Laws of 2019, most of which took effect on Oct. 23 (the security requirement provisions take effect March 21, 2020). It presents new regulation that the government of New York create to apply other regulation that is not cover under HIPAA and also include the application of criminal offenses due cybersecurity attacks	New legal regulation
Scarbecz, M., & DeSchepper, E. (2018)	Details of a study with first year dental students and the reported levels of knowledge about IT topics including cybersecurity.	Knowledge of Cybersecurity
Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019)	The study leverages a methodology to create an analyzable dataset describing newly marketed medical devices. They found that cybersecurity content in the devices remains rare.	Knowledge that cybersecurity content in medical devices remains rare.
Wirth, A. (2018)	A study of reporting some cyber incidents examples and how the healthcare sector will need to be prepare.	Cybersecurity incidents in the healthcare sector

CONCLUSION AND LIMITATIONS

Literature provides fundamental evidence of studies that help organizations establish corresponding planning, solutions, and best practices for current or new problems that will confront. The Healthcare industry has vast literature related to cybersecurity, data breaches, ransomware, cyber-attacks, but there is a lack of literature related to a specific medical practitioner, in this scenario for dental practitioners. Cybersecurity in healthcare is enormous and there is a different tendency to approach the topic in a general manner. Specific literature for small practitioners will collaborate or expand the knowledge base and solutions that will help the reduction of cybersecurity threats or data breaches. In our findings, this systematic literature review confirms the necessity to expand the amount of academic literature of cybersecurity for dental practitioners and consideration of creating a model solution that will help other small medical practitioners. Studies confirm that education aids in less cyber threats. An academic paper is an education tool not only for students, furthermore for practitioners. Future research in this topic should include the developing of a cyber resilience model, the expansion of the cybersecurity knowledge best practices and the understanding of a holistic view as a complete panorama of the cybersecurity in dental healthcare and the corresponding comply of HIPAA and HITECH.

There were some limitations that the researchers encountered in their study. First, there were a few academic articles about the subject. This resulted in limited search results. Second, cybersecurity is a broad topic. It was difficult to identify external and internal threats and trends, specifically in the dental healthcare sector. Third, the study only uses four databases. The researchers did not use additional databases available at the university. Finally, the study focused geographically on the American healthcare system and limited the search for the last 10 years. Only articles relevant to the U.S. health, that includes the Puerto Rico health system, were included in the study.

REFERENCES

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, 24-35.

Can, F. C. Y., & Avoid, S. (2019). Cybersecurity in the Dental Office: Five Cyber-Pitfalls You Can (and Should) Avoid. *Dental Assistant*, *88*(6), 16–17.

Coller, K. (2019). *Hundreds of dental offices crippled by ransomware attack*. CNN. https://edition.cnn.com/2019/08/29/politics/ransomware-attack-dental-offices/index.html

Coventry, L., & Branley-Bell, D. B. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*(2018), 48–52.

DHHS Office for Civil Rights | HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. (n.d.).

Efe, A., & Calik, E. (2018). Holistic Security Architecture for Effective Management of Healthcare Cyber Threats. *International Journal of Health Management and Strategies Research*, *4*(2), 150–167.

Health Care Industry Cybersecurity Task Force - Office of the Assistant Secretary for Preparedness. (2017). *Report on improving Cybersecurity in the Health Care Industry*. *June*, 96. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Health Industry Cybersecurity Practices: Managing threats and protecting patients. (2017). https://www.mendeley.com/catalogue/ebc43771-7582-3a39-91f3-a2f0f355ae45/

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. (2005)

Can electronic medical record systems transform health care? Potential health benefits, savings, and costs', *Health Affairs*, *24(*5), 103–1117.

HIPAA Journal - News and articles about HIPAA. (n.d.). Retrieved February 23, 2020, from https://www.hipaajournal.com/

HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

HITRUST Alliance. (n.d.). Retrieved February 15, 2020, from https://hitrustalliance.net/

Hoffman, L. J., Burley, D., & Toregas, C. (2011). Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce. *IEEE Security and Privacy*, 1–13.

Symantec. (2019). *ISTR Internet Security Threat Report 2019, 24*(1).

Kalenderian, E., Walji, M., & Ramoni, R. B. (2013). "Meaningful use" of EHR in dental school clinics: how to benefit from the U.S. HITECH Act's financial and quality improvement incentives. *Journal of Dental Education*, *77*(4), 401–415.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.

Lisbon, S. (2018). *A Comparative Analysis of HIPAA Security Risk Assessments for Two Small Dental Clinics*. 11–13.

Loughlin, S., Fu, K., Gee, T., Gieras, I., Hoyme, K., Rajagopalan, S. R., … Wirth, A. (2014). A roundtable discussion: Safeguarding information and resources against emerging cybersecurity threats. *Biomedical Instrumentation and Technology*, *48*, 8–17.

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*(March), 57–68.

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector. *International Journal of Business and Social Research*, *5*(2), 55–66.

Office for Civil Rights (OCR) HHS.gov. (n.d.). Retrieved February 15, 2020, from https://www.hhs.gov/ocr/index.html

Ortiz-de-Mandojana, N., & Bansal, P. (2016). The long- term benefits of organizational resilience through sustainable business practices, *Strategic Management Journal*, *37*(8), 1615-1631.

Plunkett, L. (2019). Erecting a Shield against the Bad Guys. *New York State Dental Journal, 85*(6), 4–7.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 2409–4285. www.IJCSSE.org

Scarbecz, M., & DeSchepper, E. (2018). Trends in First-Year Dental Students' Information Technology Knowledge and Use: Results from a U.S. Dental School in 2009, 2012, and 2017. *Journal of Dental Education*, *82*(12), 1287–1295.

Singh, R. P., A., C., Bhat, N., & Pawar, A. (2019). Perception of dental and medical teaching faculty regarding mobile dental application. *Journal of Pharmacy and Bioallied Sciences*, *11*(3), 530–539.

Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: An analysis of FDA product summaries. *BMJ Open*, *9*(6), 1-7.

Wirth, A. (2018). The times they are a-changing': Part one. *Biomedical Instrumentation and Technology*, *52*(2), 148–152.