https://doi.org/10.48009/4_iis_2019_27-34

Issues in Information Systems
Volume 20, Issue 4, pp. 27-34, 2019

HEALTH SERVICES AT RISK: AN UNANTICIPATED OUTCOME OF THE NEED FOR CYBERSECURITY

Susan G. Helser, Central Michigan University helse1s@cmich.edu

ABSTRACT

The need for cybersecurity extends across disciplines. The lack of sufficient numbers of cybersecurity specialists to fill existing and expected positions is a growing concern. Cybersecurity represents a substantive and ever-changing collection of issues that can have life-long or perhaps life-threatening consequences. Cybersecurity specialists who also possess in-depth knowledge of another area where expertise is mandatory such as in healthcare are in short supply. In the medical industry as well as in a host of other businesses cybersecurity specialists must protect systems and data. They must also maintain regulatory compliance. The importance of this work cannot be over-stated. In order to head-off the brewing crisis of a shortage of cybersecurity-medical professionals in the healthcare industry that has the potential to force the need to limit access to services, action must be taken. The threat of having to close medical facilities is real. The work here is designed to address this crisis. The study examines the shortage of cybersecurity-medical professionals, the potential impact that the deficit has on availability to healthcare, and to offer a possible solution that could produce relief to the problem.

Keywords: Cybersecurity, Healthcare, Health Insurance Portability and Accountability Act (HIPPA), Patient Information, Hacking, Medical Devices, Internet of Things (IoT)

INTRODUCTION

Cybersecurity requirements cross multiple disciplines. The shortage in *cybersecurity specialists* needed to fill existing positions is growing. *Cybersecurity* readiness requires attention to continually changing threats. Some threats have the potential to create life-threatening consequences. *Cybersecurity specialists* who also have specialized knowledge in another field such as healthcare are in high-demand and in short-supply. In the medical field not only do systems and data need to be protected, but businesses must also remain compliant with current law. It is imperative that work be done to address the deficit in *cybersecurity-medical professionals*. An unforeseen consequence of the lack of specialists to fill these positions is the forced closure of medical facilities in order to avoid issues of non-compliance. This action puts patients at risk. It is also a serious ethical concern. The focus of this study is to examine the shortage of *cybersecurity-medical professionals* in healthcare, the impact that the issue has on access to medical treatment, and to recommend a possible solution that could supply relief.

In today's digital society an individual's *digital identity* or *digital footprint* allows access to numerous diverse relationships. Activities include services such as online transactions, credit card purchases, social media, employment applications, access to legal records and email. If the Internet is available, essentially, many resources can be accessed. An individual's *digital identity* in the *digital space* is dependent on *personally identifiable information* (PII). PII is the key used to authenticate an individual on countless systems. It allows a person to tap resources that are uniquely available to her or him. PII consists of extensive data associated with an individual such as name, date of birth, gender, age, address, employment history, family relationships, educational background, insurance information, licenses, patient data, and financial records. *Smart-technologies* in combination with the *Internet of Things* (IoT) facilitate users' ability to connect electronically to online services 24/7. PII is also readily available with a few screen-touches, mouse-clicks or key-strokes. *Digital access* offers a host of conveniences that can expedite routine procedures. For example, efficiency increases as the time required to complete a task is decreases. However, the benefits realized come with a cost. *Digital access* can provide *fraudsters* with exploitable vulnerabilities. Computer networks are the avenue travelled by *digital data* for better or for worse. (Paulsen, Hazlett, Schwartz, September 2018)

Sufficient resources need to be in place to defend against attack. Otherwise, data is at risk. The consequences of a data breach include the loss of information that can extend to devastating events in the lives of individuals.

Cybersecurity and Ethical Concerns

The explosion of *e-commerce* moving across the Internet-Super-Highway is driven by the growth and expansion of technical advances in digital infrastructure. Mobile-platforms provide roads to deliver information virtually anywhere that is accessible to the Internet. Significant growth in related emerging technologies affords real benefits in the way of easy access to services. As a result of improvements in infrastructure and ongoing research that supports hand-held and other integrated devices, many former barriers to experts in the field and to time-sensitive data has been eliminated. One example that is changing the lives of people around the world is *e-medicine*. Whether the patient is a soldier on the battlefield, a person travelling in an ambulance from the scene of an accident to get help, someone on a gurney moving through the halls of a medical facility, or an individual with a pace-maker sitting at home, medical data is transferred and accessible in nearly real-time. Information that at one time was stored only on paper in folders in medical offices has been digitized and now resides in the digital realm. The convenience comes with a very real cost, since the transmission of data over vast networks is a significant lure to *hackers*.

Evolving at the same time as technical advances and the benefits related to them is the increasing opportunity of compromise. Breaches to systems that result in the access of data to *nefarious actors* are reported all too regularly and in great numbers. (Lord, June 2018) In recent years, it has become commonplace to learn of attacks at major organizations. Businesses have long been the target of *cyber criminals.* Cities such as Atlanta and Baltimore have come under attack by these individuals.(Hutcherson, March 2018, Moscaritolo, May 2019) *Identity theft, phishing ransomware, malfeasance,* and *espionage* represent just a few of criminal acts perpetrated by *fraudsters* and *hackers* who serve themselves at the expense of society. Their work shows no sign of decreasing, but rather is increasing at a significant rate.

A consequence of our evolving *digital-age* is the easy with which and speed that PII and *privacy* are lost. Their compromise relates to technical and non-technical issues. Until recently, laws that are on the books to protect individuals were often far behind the times. The problem that remains is how to address the aftermath of a *cyberattack*. Laws are written for the purpose of protection, but unforeseen results create new challenges.

Procedures and policies designed to be proactive to protect data and systems are an avenue of defense. For example, the *Confidentiality, Integrity and Availability Triad* (CIA Triad) is one model with a focus on data protection. The tree components have distinct purposes. *Confidentiality* guarantees that only authorized users can access the data so that it remains private. *Integrity* guarantees that the data is unadulterated and, therefore, can be trusted to be true. *Availability* guarantees that the data is ready for use when it is needed. (DoHS)

Cyberethics is another area of concern that directly impacts people and requires attention. Ethics needs to be embedded from the start in the design phase of systems. Consideration should be paid to all activities that involve *e-transactions*. This means that technical and non-technical issues need to be addressed. Laws such as HIPPA are in place to protect of patient records, in part for ethical reasons. However, more needs to be done in the vast *digital-age.* Recent examples such as *hackers'* attacks on retailers, schools, insurance companies, and financial institutions put individuals' PII at risk. Also, cases that involve social media companies knowingly profiting from making users' PII available to third-party agents is a transgression. Whether exploitation of data is engineered by *fraudsters hacking* into systems or the result of sale of data for marketing purposes, trust is violated. Ethics was not part of the equation. The integration of ethics from the design phase through implementation phase would help to protect data. The investment of additional resources to keep *fraudsters* out and to consider the well-being of users before profit would benefit individuals. Risk analysis in conjunctions with economic considerations need to be assessed, but ethics must be part of the solution.

Technical solutions can help to combat attacks from the outside or to monitor threats from the inside. However, an ever-growing number of *cybersecurity specialists* are needed to serve as defenders. The shortage is real and has significant repercussions. Unfilled positions are in the hundreds of thousands in the United States. (Cyber Seek) World-wide the number increases to the millions. Governments across the globe are promoting *cyber education* at the pre-college level to boost interest in *cybersecurity* as a career in an attempt to help fill the pipeline. In spite of these efforts, the number of individuals who are needed exceeds existing pool. Projections are that the deficit in talent

will continue to increase. The question becomes, "What will be done when no one is available to do the required work?" An insufficient number of *cybersecurity specialists* in fields such as healthcare have *ethical* consequences tangentially related to the shortage along with those outlined earlier. We will consider a case in point in the next section.

PROBLEM STATEMENT

The imperative to protect patient data in healthcare is two-fold. It includes ethical concerns as well as legal mandates. As is the case across multiple disciplines, the shortage in number of appropriately trained *cybersecurity specialists* is critical. Hundreds of thousands of *cybersecurity* positions are unfilled in the United States. Worldwide the number of individuals who are needed to fill jobs is in the millions. The deficit in talent is increasing with the evolution of the *digital-age*. *Cybersecurity specialists* must address issues that range from purely technical, such as hardware or software based problems, to those that encompass policy. Individuals with expertise are needed across the spectrum. *Cybersecurity specialists* in healthcare must also possess extensive medical knowledge in order to successfully complete work that is required. This added requirement creates a layer of challenges, but also affords opportunities. Statistics illustrate the issue.

The healthcare industry is a fertile ground with numerous vulnerabilities for *fraudsters* to exploit. Information breaches directly affect the confidentiality and security of patient records. (Bhimji, Hackert, January 2018; Coventry, Branley, April 2018; Bachiri, Idri, Fernández-Alemán, Toval June 2018; Baranchuk, Alexander, Campbell, Haseeb, Redfearn, Simpson, Glover, September 2018; Paulsen, Hazelett, Schwartz, September 2018)

Federal Law mandated in HIPAA requires data protection. (Edemekong, Haydel, January 2018; Cohen, Mello, July 2018) Proposed hardware and software solutions to address the diverse challenges in the healthcare field continue to be developed. Critical to meeting industry needs to protect patient data, medical devices and sensitive healthcare systems are professionally trained *cybersecurity-medical specialists*. (Adams-Collman, March 2018; Chen, Ge, Moore, Yang, Li, Proctor, June 2018; Cohen, Mello, July 2018; Mozzaquatro, Agostinho, Goncalves, Martins, Jardim-Goncalves, September 2018; Levitin, Xing, Huang, October 2018)

Table 1 lists the *Top 10* healthcare data breaches as per the United States Department of Health and Human Services Office for Civil Rights in millions of people affected from least to greatest. The years represented in Table 1 span 2011 through 2016. Another alarming statistic determined in a 2017 survey conducted by *Accenture* showed that more than a quarter of the citizens of the United States, (26%), have been impacted by data breaches in the healthcare industry. Of the people whose medical records were compromised, 50% experienced *identity theft* that resulted in an average loss of $2,500 of out-of-pocket expenses related to the crime. (Lord, June 2018)

Table 1. Top 10 Medical Data Breaches in Millions, Least to Most (Lord, June 2018)

Rank	Business	Affected	Month(s)	Year
10	NewKirk Products	3.47	Aug	2016
9	Banner Health	3.62	Aug	2016
8	Medical Informatics Engineering	3.9	July	2015
7	Advocate Health Care	4.03	Aug	2013
6	Community Health Systems	4.5	Apr-Jun	2014
5	University of California, Los Angeles Health	4.5	July	2016
4	TRICARE	4.9	Sep	2011
3	Excellus BlueCross BlueShield	10+	Sep	2015
2	Premera Blue Cross	11+	Jan	2015
1	Anthem Blue Cross	78.8	Jan	2015

During a recent meeting with the Chief Information Security Officer (CISO) of a third-party healthcare *cybersecurity provider*, a severe problem that affects the industry came to light. The need for *cybersecurity-medical specialists* has reached a critical point. Every healthcare facility must employ individuals with the appropriate combination of skills. However, *cybersecurity-medical specialists* are in short supply. In addition to the understood responsibilities associated with work required of a *cybersecurity professional* to protect business data and computer systems, *cybersecurity-medical specialists* must also oversee the *cyber* concerns related to HIPAA compliance. The work requires extensive knowledge of *cybersecurity* and healthcare in order to do the job. At this time, locating employees with the necessary combination of expertise poses significant challenges.

The conversation revealed a distressing, ethically thought-provoking and very likely life-threatening outcome of the shortage of *cybersecurity-medical specialists.* The CISO reported that after a major regional healthcare provider purchased a hospital in a rural community, the provider was forced to close the facility for a period of time, because a *cybersecurity-medical specialist* was not employed at the site. The hospital remained shut until an individual with appropriate medical knowledge was hired and received *cybersecurity* training. In the interim, people living in the area were without a hospital and the emergency services that it can provide. The mandate for data protection and compliance through *cybersecurity* was instrumental in this ethical quandary.

The CISO continued by stating that extensive opportunities in healthcare exist for *cybersecurity-medical specialists.* Further, these opportunities are not limited to rural environments. In fact, they represent a significant problem across the healthcare industry. According to the CISO, every medical facility must have employees with the proper *cybersecurity-medical* training. When asked what the expected compensation would be for an individual with the appropriate *blended* credentials, the CISO indicated that the salary range is $75K-$115K.

Our initial research supports the assertion made by the CISO that a critical shortage of *cybersecurity-medical specialists* exists. Demand is high. Reported salaries fall in the range stated by the CISO. We are in the process of conducting a survey to determine the current need of *cybersecurity-medical specialists* in healthcare. In addition, we are examining the future potential for employment in this area of healthcare.

FUTURE DIRECTIONS

The solution that we recommend is the creation of an educational track to prepare individuals for a career as a *cybersecurity-medical specialist.* Students could decide to pursue this path as a first-choice for employment. However, the *cybersecurity-medical specialist* could provide a career option for any individual with prior medical knowledge who wants to continue in healthcare, nut move in a slightly different direction.

The number of students who graduate from nursing programs has increased, particularly in BSN programs. However, the shortage of clinical sites, classroom space, qualified teaching faculty, budget constraints and other issues has created a learning environment with insufficient capacity to educate the number of highly qualified applicants. As a consequence, many are turned away. (Buerhaus, Auerbach, Staiger, February 2016; FactSheet, May 2017; Kavilanz, April 2018; Mozzaquatro, Agostinho, Goncalves, Martins, Jardim-Goncalves, September 2018; Salsberg, April 2015)

The *cybersecurity-medical specialist* provides a great alternative career option for highly qualified students who were not accepted into nursing programs. Our intention is not to recruit students away from nursing. A significant shortage a graduates already exists in that field. However, we suggest drawing on the valuable resource pool that is the result of the existing nursing education system. Students in this pool who opt to pursue additional education in *cybersecurity* could provide relief to address the need for *cybersecurity-medical specialists.* We will consider reported statistics that support this direction.

Data in Figures 1 and 2 reveals that the capacity problem in nursing education has continued over a period of time. Figure 1 shows the *Percentage of Nursing Programs that Did Not Admit Qualified Applicants by Program Type in 2012 and 2014*. As stated earlier, the reason nursing programs turn away highly qualified applicants is due to the significant lack of capacity that exists. Figure 2 shows the *Percentage of Qualified Applicants Not Admitted by Program Type in 2012 and 2014*. Data in this chart represents the number of highly qualified applicants who were not admitted to nursing programs, due to the lack of capacity. The information in both graphs is alarming, since

projections suggest that the need for nurses is growing as baby-bombers age. (FactSheet, 2017) The graphs speak for themselves and reflect the troubling bottleneck that exists in nursing education.

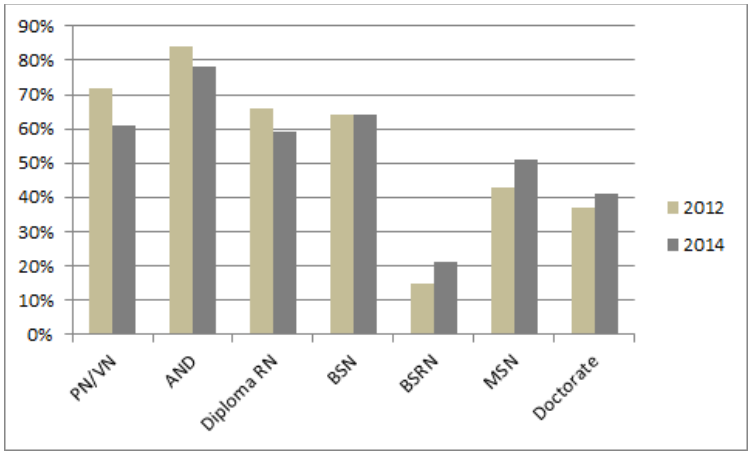

Figure 1. Percentage of Nursing Programs that Did Not Admit Qualified Applicants by Program Type during 2012 and 2014 (National League of Nursing, 2015)

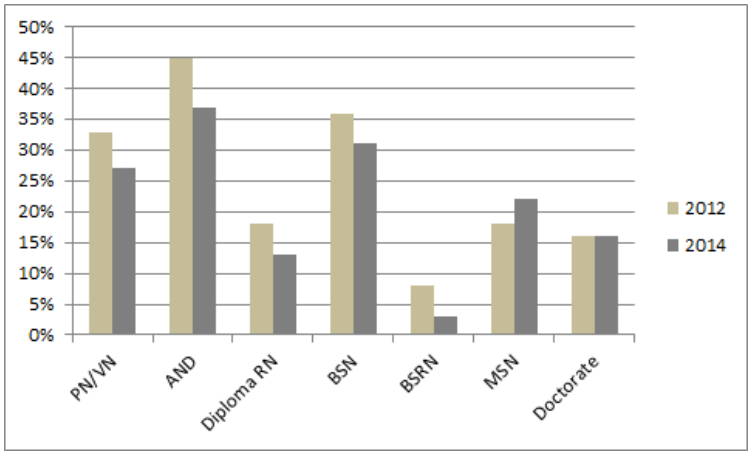

Figure 2. Percentage of Qualified Nursing Applicants Not Admitted by Program Type during 2012 and 2014 (National League of Nursing, 2015)

The American Association of Colleges of Nursing report *2016-2017 Enrollment and Graduations in Baccalaureate and Graduate Programs in Nursing* states that nursing schools in the United States turned away 64,067 qualified applicants from baccalaureate and graduate nursing programs in 2016. Reasons given for not admitting these students included insufficient resources needed to educate them such as lack of faculty, clinical sites, clinical preceptors, classroom space, and budget constraints. Nearly two-thirds of the nursing schools indicated on the survey that the primary reason for the problem of capacity was due to not enough qualified faculty and/or clinical preceptors. (Fact Sheet, 2017) Figure 3 reports the *Number of Qualified Applicants to Nursing Programs Turned Away Between 2007 and 2017.* As reported, the trend is relatively steady over a period of years.

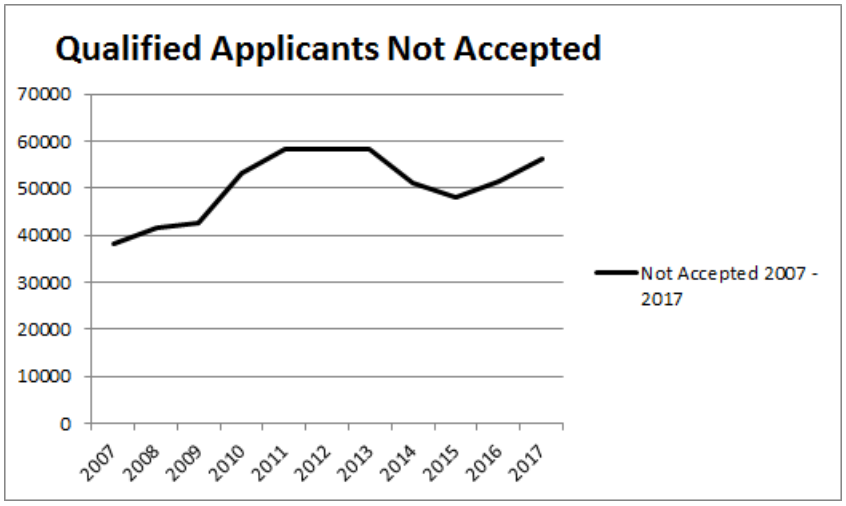

Figure 3. Number of Qualified Applicants to Nursing Programs Turned Away Between 2007 and 2017 (Kavilanz, April 2018)

In excess of 56,000 qualified nurse applicants were turned away in 2017. Statistics from a number of nursing programs reveals a significant shortage of available educational resources to support highly qualified applicants who want to become nurses. Given pools of 343, 262 and 200 highly qualified applicants, 60, 60 and 55 were accepted, respectively. Out of the pool of more than 800 qualified applicants less than 200 were admitted to a program, approximately just 22%. This is in spite of the disturbing deficit of nurses in healthcare. (Kavilanz, April 2018)

Rather than considering the pool of applicants not accepted into nursing programs as a negative, we look at this group as a positive resource. For those students who want to remain in healthcare and are so inclined, we propose the alternative career option of *cybersecurity-medical specialist.* This career choice is a critical component in today's healthcare system. The work is in high demand, requires solving challenges, and can provide an adequate living wage. As a *cybersecurity-medical specialist,* graduates will directly impact the critical need for people in this area of healthcare. Most importantly, individuals who shift from one career to the other will help to make it possible for medical facilities to remain open in the community.

Our solution taps into a pool of highly qualified applicants, who after being turned away, for all intense purposes have little hope of pursuing their initial career choice. Students in this group are well-prepared. They have GPAs of 3.5 or greater along with solid credentials in community service. They represent excellent candidates for an alternate career as a *cybersecurity-medical specialist*. Shifting these students to different area in the healthcare industry is straightforward. They need to complete several courses in *cybersecurity*. Once the coursework is finished, students would be ready to step into a challenging position as a *cybersecurity-medical specialist*. Further, as a result of current constraints that exist in nursing programs, the pool of highly qualified applicants who were turned away and who might consider a career as a *cybersecurity-medical specialist* seems likely to remain strong for the foreseeable future. (FactSheet, May 2017; NLN Findings, 2015; Kavilanz, April 2018)

In addition, we are preparing a survey to assess the potential size of the candidate pool who might consider an alternate career as a *cybersecurity-medical specialist.* Included in the group are highly qualified applicants to nursing programs who were turned away, due to a lack of capacity in the educational system. In addition, it is our understanding that another possible pool of candidates exists who possess extensive medical training. This group of highly qualified students intended to pursue careers in physical therapy, but because of constraints that mirror those in nursing they were turned away. Some of these students might consider shifting from an initial career choice as a physical therapist to working as a *cybersecurity-medical specialist.* We are in the process of researching the size this pool of candidates as well.

The option that we suggest offers an alternative career path to students who made the choice to work in healthcare, but who were not accepted into a nursing program. While not all highly qualified applicants to nursing programs or other programs such as physical therapy who were rejected will decide to shift to *cybersecurity,* some will. The option of *cybersecurity-medical specialist* represents a good opportunity for students. The increase in professionals in this area will benefit medical facilities that require the protection of patient data, equipment, and compliance with Federal Law. Our recommendation does not negatively impact the field of nursing. We do not advocate a course of action that would reduce the pool of nursing applicants. Rather, our solution draws from a valuable existing resource pool that is the result of current nursing programs. Our proposed direction represents a win for everyone.

RESULTS

Currently, we are examining a number of directions to support the creation of an educational track to provide the combined *cybersecurity* and *medical* knowledge required in healthcare. Initiatives include collaboration across schools within our University as well as developing external partners at other institutions. Also under consideration are potential additional resource pools of students who were turned away from medical programs such as physical therapy. To examine this possibility we are preparing a survey to request data from colleges and universities that offer healthcare programs to request data on the number of highly qualified applicants who were not admitted to programs. We are also polling medical facilities to assess the number *cybersecurity-medical specialists* who are required and where they are most needed. Finally, we intend to share our research with other institutions with the hope to increase the number of *cybersecurity-medical specialists*. The need is great. Moving in positive directions to mitigate this growing problem is critical.

SUMMARY

Career opportunities as *cybersecurity-medical specialists* offer rewarding work in the field of healthcare. Responsibilities are diverse and include the need to protect patient data, secure key infrastructure and maintain compliance. The critical shortage in the number of individuals who are ready to address these challenges is a cause for concern. It represents a growing vulnerability on multiple fronts in the field of healthcare. We offer a possible avenue to address this escalating problem. Given their strong interest and preparation in healthcare, in part due to a solid earning potential, the career of *cybersecurity-medical specialist* is an exceptional alternative for highly qualified students who were not admitted into nursing programs or related areas. Not every applicant who was turned away will opt to move in a different direction work in *cybersecurity.* However, those who do will help to reduce the critical shortage of *cybersecurity-medical specialists* in healthcare. It is our sincere hope that *cross-disciplinary* programs are developed that provide students with the information that they require to pursue careers as *cybersecurity-medical specialists*. The need for these professionals is great. Once in the workforce, they can make a difference. Work to address the deficit in *cybersecurity-medical specialists* will benefit all parties. Students, medical facilities, and the community will all win.

REFERENCES

Adams-Collman, J. (2018). Ransomware and Cyber Security: the King That Did Not Wannacry. *Primal Dental Journal, 7*(1), 44-47. doi: 10.1308/205016818822610307.

Bachiri, M., Idri, A., Fernández-Alemán, J. L., Toval, A. (2018). Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring. *Journal of Medical Systems, 42*(8), 144. doi: 10.1007/s10916-018-1002-x.

Baranchuk, A., Alexander, B., Campbell, D., Haseeb, S., Redfearn D, Simpson C, Glover B. (2018). Pacemaker Cybersecurity. *Circulation, 138*(12), 1272-1273. doi: 10.1161/CIRCULATIONAHA.118.035261.

Buerhaus, P., Auerbach, D., Staiger, D. (2016). *Recent Changes in the Number of Nurses Graduating from Undergraduate and Graduate Programs,* Nursing Economic 34(1).

Bhimji, S. S., Hackert, P. B. (2018). Patient Confidentiality, StatPearls [Internet]. Treasure Island, FL: StatPearls Publishing.

Chen, J., Ge, H., Moore, S., Yang, W., Li, N., Proctor, R. W. (2018). Display of Major Risk Categories in Android Apps. *Journal of Experimental Psychology Applied, 24*(3), 306-330. doi: 10.1037/xap0000163. Epub 2018 Jun 21.

Cohen, I. G., Mello, M. M. (2018). *HIPAA and Protecting Health Information in the 21st Century*, JAMA. 320(3), 231-232. doi: 10.1001/jama.2018.5630.

Coventry, L., Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22.

Cyber Risks to Next Generation 911, United States Department of Homeland Security (DoHS), https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20FINAL%20508C%20%28003%29.pdf

Cyber Seek, https://www.cyberseek.org/

Edemekong, P. F., Haydel, M. J. (2018). *Health Insurance Portability and Accountability Act (HIPAA),* StatPearls [Internet]. Treasure Island, FL: StatPearls Publishing.

Fact Sheet: Nursing Shortage, *American Association of Colleges of Nursing*, www.aacnnursing.org, May 2017

Findings from the 2014 NLN Biennial Survey of Schools of Nursing Academic year 2013-2014: executive summary. (Headlines from the NLN) (National League of Nursing) (2015). *Nursing Education Perspectives, 36*(6), 425(2)

Hutcherson, K. (2018). Six Days After a Ransomware Attack, Atlanta Officials are Filling Out Forms By Hand, March 2018, https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html

Kavilanz, P. (2018). *Nursing schools are rejecting thousands of applicants – in middle of a nursing shortage,* https://money.cnn.com/2018/04/30/news/economy/nursing-school-rejections/index.html

Levitin, G., Xing, L., Huang, H. Z. (2018). *Security of Separated Data in Cloud Systems with Competing Attack Detection and Data Theft Processes.*, *Risk* Anal. 2018 Oct 12. doi: 10.1111/risa.13219. [Epub ahead of print]

Lord, N. (2018). *Top 10 Biggest Healthcare Data Beaches of All Time,* DigitalGuardian, June, https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

Moscaritolo, A. (2019). *Ransomware Attack Strikes Baltimore City Government,* May, https://www.pcmag.com/news/368231/ransomware-attack-strikes-baltimore-city-government

Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., Jardim-Goncalves, R. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things, *Sensors (Basel), 18*(9), E3053. doi: 10.3390/s18093053.

Paulsen, J. E., Hazelett, M., B., Schwartz, S. B. (2018). CIED Cybersecurity Risks in an Increasingly Connected World. *Circulation, 138*(12), 1181-1183. doi: 10.1161/CIRCULATIONAHA.118.035021.

Salsberg, E. (2015). *Recent Trends in the Nursing Pipeline: US Educated BSNs Continue to Increase,* April, https: //www.healthaffairs.org/do/10.1377/hblog20150409.046241/full/