**Review Article**

**Is Public Health Playing Checkers or Chess with Public Health Data**

**Mark McKinney, EdD#**

College of Health and Human Development, The Pennsylvania State University, Pennsylvania, USA

**#Corresponding authors:** Mark McKinney, EdD, Assistant Teaching Professor, College of Health and Human Development, The Pennsylvania State University, 604Q Ford Building, University Park, Pennsylvania 16802, USA

**How to cite this article:** McKinney M (2022) Is Public Health Playing Checkers or Chess with Public Health Data. Int J Comm & Publ Healt 02(01): 2021-08.

**Submission Date:** 17 September, 2021; **Accepted Date:** 11 January, 2022; **Published Online:** 16 January, 2022

**Abstract**

This article contains opinions on how public health professionals and organizations managed their public health information from the Covid-19 pandemic. Given the current Covid-19 pandemic and the importance of the information obtained by public health organizations and professionals, protecting the Information Technology (IT) systems and networks housing this important information is important. With public health organizations and professionals revising past pandemics whereas IT was not highly involved, applying a chess-like thinking approach opposed to the current checkers-like strategic thinking and planning needs to be employed. During this research, an analysis of the IT systems and applications utilized throughout the Covid-19 pandemic is explored. Further, defining aspects of cybersecurity and strategic planning through managing public health IT systems and networks is identified and applied to the situation.

**Keywords:** Covid-19; Information Technology; Pandemic; Public Health; Strategic Planning

**Introduction**

In reviewing public health data, an analogy of checkers and chess is easily relatable as both games require strategic thought and analytical skills. Much like protecting public health data, chess and checkers requires a certain level of strategic design to ensure a successful outcome. Ultimately, the object of checkers is simply to capture or trap the opponent’s game pieces, however, the game of chess necessitates more complexity and demands increased strategic thinking and focus. In light of the Covid-19 pandemic and its associated public data, public health officials and organizations need to employ a chess-like strategy opposed to a checkers-like one when managing public health Information Technology (IT) systems and networks.

As the collective world deals with the global Covid-19 pandemic, public health professionals a vital responsibility to minimize the global impact of such an event in the future. Without question, pandemics are considered anticipated consequences given current overpopulation in many major city centers over the world; therefore, managing public health data must be equally anticipatory. This article focuses on aspects of managing public health data during the Covid-19 pandemic and the strategy employed with managing and securing the IT systems and networks that maintain public health data. At the onset of the Covid-19 pandemic in March 2020, close to 10 million cases were confirmed with almost 500,000 recorded deaths. The importance of this data surely aided to reducing future pandemic associated illnesses and deaths; however, how was this data protected to sustain its integrity [1]? Furthermore, given the immediacy and urgency of the pandemic, solely utilizing an IT system and network to maintain and protect this important data was not sufficient. There were several reports and studies regarding the utilization of IT technologies during the COVID-19 outbreak for diagnosis, statistical reporting, monitoring and controlling disease, forecasting, etc. [2,3]; however, in these studies, no emphasis was placed upon the security of the IT systems or network utilized by public health organizations.

**Information Technology Utilization**

The Covid-19 pandemic and its effect on public health worldwide has proven monumental to global operations; however, so too is managing its data an enormous task in the current post-pandemic environment. During the height of the pandemic, digitizing the collective information on the various Covid-19 viral strains proved challenging at best for public health professionals. Although many organizations took steps to secure Covid-19 public health information, the action of ensuring the security of this information required more rigorous IT security for public health systems and networks than initially thought [4]. The Covid-19 pandemic increased demand for innovative solutions to manage the copious amount of public health data through non-standard practices [5,6]. Primarily, because of the Covid-19 pandemic, public health professionals and organizations have utilized mobile devices (and apps), tele-health, telemedicine, Internet of Things (IoT) and associated information technology systems to manage an excessive amount of data [6,7,8].

The Covid-19 pandemic should serve as the IT system procurement tool for public health organizations in that current processes are not sustainable. Prior to the pandemic, utilization of healthcare technological services saw an increase that indicated the importance of having such technology available for patients. The 2010-2017 timeframe provided insight into how important technology was in that U.S. hospitals served patients from 35% to 76% percent of appointments. Furthermore, as pre-pandemic numbers remained consistent throughout all healthcare specialties utilizing these services, it was anticipated that a significant utilization increase would not startle the healthcare industry.

At the start of the pandemic, public health organizations appeared prepared to handle the transference to remote operations; however, initial estimates were inaccurate as internet services increased an estimated 40% to 100% opposed to the pandemic [9]. Furthermore, video-conference services, such as Cisco WebEx, Zoom, and Teams, also have increased in utilization a minimum of 35% opposed to non-pandemic rates [10]. The rapid use expansion of Zoom Cloud Meetings and Video Communications at the height of the pandemic as primary means of telecommunications, ultimately shifted to apprehensive backlash as the Zoom platform revealed its susceptibility to cybercriminal exploitation, thus raising security and privacy concerns [11].

In addition to administrative services used during the pandemic, the delivery of healthcare services via digital and internet technology increased substantially. Similar to the usage of technological services and equipment, tele-health, telemedicine and affiliated medical delivery services increased tremendously during the pandemic. Since pandemic inception, Telemedicine Services (TMSs) became a critical asset across the entire U.S. health care delivery spectrum, with an increase from 35% to 76% [12]. Through the adaptation of mobile technology, pandemic assistance technology advanced significantly through Twitter, which provided public health organizations a powerful tool for rapid and direct communication on COVID-19 to citizens, opposed to conventional media [13].

**Cybersecurity and Public Health**

The Covid-19 pandemic, unfortunately, has been a red alert that public health officials and organizations were ill-prepared to address and secure public health information; which included Covid-19 and non Covid-19 information. For public health organizations, maintaining the security of public health data ultimately leads to new pandemic remedies and may save lives; however, for cybercriminals, it is another opportunity to make money or inject their political perspective. Cybercriminals, usually individuals or organizations, conduct illegal activities on public health information systems to steal, exploit, or compromise network integrity [14]. Through all the chaos associated with adjusting to the pandemic, many public health professionals were focused on controlling Covid-19, when the information and data contained within public health systems and networks should have received equal attention.

Public dependency on information technology increased dramatically with the spread pandemic inception and there is no sign of technological usage declining. As usage continues to increase, so too will cyber threats. According to the 2020 Official Annual Cybercrime Report []15,16], “Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind” [16] and ultimately will have a global price tag in excess of $6 trillion annually by the end of 2021 [15]. Given the urgency of preventing cybercrime, it is prudent to inquire about what public health organization have done to prevent cybercrime? Well the answer to the aforementioned question is, very little, which clearly placed public health organizations in a vulnerable position.

In similar fashion to other organizations when the Covid-19 pandemic was in full swing, organizations scrambled to adapt and forced organizations to view their internal adaptation protocols. When public organizations completed their internal review, they quickly realized they were not immune and were like most organizations without a plan to facilitate immediate and drastic change with limited or minimal time [17]. Therefore, without a contingency plan to deal with protecting the data associated with Covid-19, public health organizations essentially were vulnerable to cyber-attacks regarding critical information needed to end the pandemic.

As public health officials discovered that protecting Covid-19 public health information was essential and historical practices proved insufficient as cybercriminals advanced their assault on healthcare by attacking public health departments. One such example was the Champaign-Urbana Public Health District, that was hit with a ransomware attack on the system that housed the district’s Covid-19 information [18]. In classic Ransomware fashion, cyber criminals obtained control of the Champaign-Urbana Public Health District network and demanded a restoration ransom, which was paid by the cyber victim. However, given the circumstances surrounding the incident, the question that needed to be asked what, could this ransomware incident be prevented? I surmise to you the answer is an emphatic yes.

In addition to increased Ransomware attacks, cybercriminals utilized other measures to include Phishing, Distributed Denial of Service (DDoS), and Malware to compromise public health organizations. In reviewing everything that has occurred to public health organizations during the Covid-19 pandemic, it is not surprising the attacks were conducted as healthcare organizations are a favorite of cybercriminals. Such an example is the WannaCry ransomware attack in 2017 that impacted the National Health Service [17].

Given that healthcare organizations are constantly attacked, reducing or eliminating vulnerabilities should be a top priority; however, this is not the case. Public health organizations (like healthcare organizations) often do not dedicate sufficient funds towards protecting their IT systems and networks. The focus is on public health issues that lead to more severe problems, such as a pandemic. Given the emphasis during the pandemic was primarily of the privacy of vaccine information, more of an emphasis should have been directed towards securing the information technology infrastructure used to house pandemic vaccine data. Rothstein [17] indicated, the utilization of health information technology during the pandemic emphasized public health policy development with an emphasis on privacy: (1) necessity and effectiveness, (2) proportionality and minimal infringement, (3) purpose limitations, and (4) justice (p. 1374). Conversely, the focus on public health information should be more aligned with organizational strategic processes to ensure information security since cybersecurity threats continue to persist.

**Strategic Planning Alignment**

Prior to the gestation of the Covid-19 pandemic, public health professionals were directly involved in applying strategic planning into their everyday processing; and in fact, public health professionals utilized strategic planning for the 2009 Influenza A (H1N1) pandemic. For many, it is hard to believe that there actually were other pandemics and sadly enough, it appears that many have forgotten that important fact. Regarding the data produced from the H1N1 pandemic, information was disseminated to public health professionals daily to ensure critical information on how to end this pandemic. The data dissemination process was within an integrated information system whereas each essential public health department obtained this information [20]. Given the situation at the time, the implementation of strategic planning into the data dissemination was essential to the pandemic being resolved; however, in looking at strategic planning for the current Covid-19 pandemic, it served as a different challenge than the H1N1 pandemic [21].

With all that public health professionals know about the Covid-19 virus and impact on the world, aligning public health and vaccine data with public health strategies can bring the end to this pandemic. However, one thing that is different from previous pandemics is the inclusion of strategic planning in managing the pandemic. As public health has evolved, so to has the demand for strategic planning through analytical reports, performance dashboards and initiatives. Along with this demand is the participation of public health strategic planners to understand the myriad of challenges of the Covid-19 virus and apply strategy in dealing with eliminating Covid-19 from the world.

An essential element is using strategic planning in managing Covid-19 is to strategically align organizational goals, objectives and mission with Covid-19 data analytics and supporting information technological processes focused on the Covid-19 pandemic [22]. When strategic alignment occurs, it creates opportunities for successful outcomes, increased leadership visibility and great information dissemination among the public at-large. It also leads to consistent evaluation of current operational procedures for a guiding framework for applying analytical and prioritization measures to current Covid-19 pandemic activities.

The application of strategic planning not only works for public health activities, but for the information technology systems public health organizations utilize. The process of Strategic Information System Planning (SISP) is one public health organizations need to implement as of yesterday. The process of utilizing the SISP aligns organizational IT strategies with other organizational strategies and goals to ensure everything is synchronized. The SISP applies five (5) steps: (1) Planning Health IT Planning, (2) Analyze Current Environment or Situation; (3) Develop Strategic Alternatives, (4) Select and Formulate Strategy, and (5) Plan Strategic Implementation [23]. For Step 1: Planning Health IT Planning-public health professionals need to investigate how current Covid-19 protocols, processes and activities are aligned with public health organizational strategic initiatives and most importantly, organizational IT networks and systems. Step 2: Analyze Current Environment or Situation-pertains to how public health Covid-19 activities are being conducted in synchronization with organizational or affiliated organizational IT protocols and data management protective measures. Step 3: Develop Strategic Alternatives-involves creating a strategic plan to address public health organizational (or affiliated) IT systems that house and manage Covid-19 data are secure against cybercriminals. Step 4: Select and Formulate Strategy-involves selecting the most appropriate strategy that ensures public health organizations are aligned and them developing an implementation strategy to ensure public health organizational processes are fully protected, to include securing IT systems and networks. Step 5:Plan Strategic Implementation-this portion of the plan is where implementing the strategy involves project management protocols to ensure everything falls in line with public health organizational (and affiliated) measures, including IT networks and systems are fully protected [23].

Contained within the aforementioned steps are opportunities for public health officials investigate and research each step through four (4) essential dimensions: Alignment, Analysis, Cooperation, and Capabilities [23]. For Dimension 1: Alignment-this is considered most important in that aligning of all public health measures, opportunities, IT systems and networks towards public health priorities leads to the protection of Covid-19 information. Dimension 2: Analysis-involves analyzing all essential information pertaining to public health activities and protocols governing Covid-19. Most importantly, it involves analyzing trends, breaches, etcetera for the public health organization. Dimension 3: Cooperation-also is equally important in that public health organizations and officials often work alongside other public health organizations and officials; therefore, it is essential that cooperation agreements are in place, to include IT system and network protections and activities. Dimension 4: Capabilities-this area is often overlooked but equally important regarding strategic alignment. All public health organizations are not created equal, therefore, if public health organizations and their IT networks and systems are not on par with each other, capabilities may be impacted and so it is essential public health organizations and officials keep this in mind when working collaboratively.

Public health organizational implementation of strategic planning is here and ever-present and so it must be taken seriously. In similar fashion to healthcare organizations and how their organizational mission, vision, values and goals are strategically aligned, so to must public health organizations ensure everything is strategically aligned. Given the current situation involving Covid-19, it is even more important since IT systems and networks are highly involved in the strategic alignment process and one is not more important than another. Through pairing IT advances, strategic alignment of organizational planning, activities and measures, places public health organizations in a position of getting ahead of future public health emergencies instead of reacting to one. It is through applying a chess-like strategy and not a checkers-like strategy, public health organizations can ensure the Covid-19 pandemic information, data and IT systems and networks remain secure.

**Moving Forward**

As the Covid-19 pandemic continues to advance globally, managing all aspects of the pandemic appears simplistic on the surface; however, it requires more attention to detail by public health professionals. Understandably, a pandemic involves a lot of public health information and it is through that information whereas associated data must take more of a spotlight. Through this spotlight, public health professionals should recognize conduct a systemic review of their system and network infrastructure by way of the following: Review, Replace, Remediate, and Revitalize [24]. Public health professionals and organizations should conduct a comprehensive review of all organizational IT systems and networks for functional security. This should identify any potential vulnerabilities to be remedied. The Replace portion involves the outcomes of the review in that anything that is not within a 1-3-year period, should be replaced to ensure all public health IT systems and networks have the necessary security infrastructure. As for Remediate, deals with addressing organizational challenges to the IT systems and networks, which may involve modification of process, policies and procedures. Lastly, revitalize addresses deals with understanding new platforms and capabilities of public health IT systems and networks. It also may involve bringing in additional personnel, such as IT professional and digital solutions that can deal with future cyber-attacks.

Ultimately, public health professionals need to face the fact that their research, vaccination, and other assorted data and information are no longer considered irrelevant to cybercriminals. Furthermore, gone are the days of the Health Insurance Portability & Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) as being the essential elements to ensuring public health safety and compliance. Public health professionals need to step out of their comfort zone and understand their information technology systems and networks are the targets of bad actors like other industries. In short, it means public health professional and organizations need to ensure they are thinking and conducting strategic planning into all aspects of operations. It means thinking three-dimensionally like a chess player and not two-dimensionally like a checkers player. It involves thinking about how they can be attacked and devise remedies to those vulnerabilities. Overall, nothing in life is guaranteed or infallible; however, public health professionals must view their organizational processes in a way that they can continue to advance in protecting critical information to sustain public health.

**References**

1. [Connor P (2020) More than nine-in-ten people worldwide live in countries with travel restrictions amid COVID-19. Pew Research Center.](https://www.pewresearch.org/fact-tank/2020/04/01/more-than-nine-in-ten-people-worldwide-live-in-countries-with-travel-restrictions-amid-covid-19/)
2. [Wang S, Kang B, Ma J, et al. (2021) A deep learning algorithm using CT images to screen for Corona vrus disease (Covid-19). European Radiology 31: 6096-6104.](https://pubmed.ncbi.nlm.nih.gov/33629156/)
3. [Asadzadeh A, Pakkhoo S, Saeidabad M, et al. (2020) Information technology in emergency management of Covid-19 outbreak. Informatics in Medicine Unlocked 21: 100475.](https://www.sciencedirect.com/science/article/pii/S2352914820306262)
4. [Feger H (2021) Securing the digital future. Community Practitioner 94: 48-49.](https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1113029)
5. [O’Leary DE (2020) Evolving information systems and technology research issues for COVID-19 and other pandemics. Journal of Organizational Computing and Electronic Commerce 30: 1-8.](https://www.tandfonline.com/doi/full/10.1080/10919392.2020.1755790)
6. [Wu H, Zuopeng Z, Wenzhuo L (2021) Information technology solutions, challenges, and suggestions for teackling the Covid-19 pandemic. International Journal of Information Management 57: 102287.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7724285/)
7. [Kumar K, Kumar N, Shah R (2020) Role of IoT to avoid spreading of COVID-19. International Journal of Intelligent Networks 1: 32–35.](https://www.sciencedirect.com/science/article/pii/S2666603020300026)
8. [Sein MK (2020) The serendipitous impact of COVID-19 pandemic: A rare opportunity for research and practice. International Journal of Information Management 55: 102164.](https://www.sciencedirect.com/science/article/pii/S0268401220308689)
9. [De R, Pandey N, Pal A (2020) Impact of digital surge Covid-19 pandemic: A viewpoint on research and practice. International Journal of Information Management 55: 102171.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123/)
10. [Branscombe M (2020) The network impact of the global COVID-19 pandemic.](https://thenewstack.io/the-network-impact-of-the-global-covid-19-pandemic/)
11. [Khan NA, Brohi SN, Zaman N (2020) Ten deadly cyber security threats amid Covid-19 pandemic.](https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792)
12. [Chauhan V, Galwankar S, Arquilla B, et al. (2020) Novel coronoavirus (Covid-19): Leveraging telemedicine to optimize care while minimizing exposures and viral transmission. Journal of Emergency Trauma Shock, Jan-Mar 13: 20-24.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7161346/)
13. [Rufai SR, Bunce C (2020) World leaders’ usage of Twitter in response to the Covid-19 pandemic: a content analysis. Journal of Public Health 42: 510-516.](https://pubmed.ncbi.nlm.nih.gov/32309854/)
14. [Chigada J, Madzinga R (2021) Cyberattacks and threats during COVID-19: A systematic literature review’, South African Journal of Information Management 23: a1277.](https://sajim.co.za/index.php/sajim/article/view/1277)
15. [The 2020 Official Annual Cybercrime Report. Herjavic Group. 2020.](https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/#:~:text=According%20to%20the%202020%20Official,the%20biggest%20problems%20with%20mankind)
16. [The 2019 Official Annual Cybercrime Report. Herjavic Group. 2020.](https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/#:~:text=According%20to%20the%202020%20Official,the%20biggest%20problems%20with%20mankind)
17. [Pranggono B, Arabo A (2020) Covid-19 pandemic cybersecurity issues. Internet Technology Letters e247. John Wiley & Sonds, Ltd.](https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247)
18. [Bergal J (2020) Hospital hackers seize upon Coronavirus pandemic. The PEW Charitable Trusts.](https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/04/13/hospital-hackers-seize-upon-coronavirus-pandemic)
19. [Rothstein MA (2020) Public health and privacy in the pandemic. American Journal of Public Health 110: 1374-1375.](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7427234/)
20. [Farias DR, Raffo L, Bacigalupo S, et al. (2010) Data for decision making: Strategic information tools for hospital management during a pandemic. Disaster Medicine and Public Health Preparedness 4: 2027-212.](https://www.cambridge.org/core/journals/disaster-medicine-and-public-health-preparedness/article/abs/data-for-decision-making-strategic-information-tools-for-hospital-management-during-a-pandemic/057B6C30E18881533F26A3A3C66AB379)
21. [Kirlin J (2020) Covid-19 Upends pandemic plan: American Review of Public Administration 50: 467-479.](https://journals.sagepub.com/doi/full/10.1177/0275074020941668)
22. [Glandon GL, Smaltz DH, Slovensky DJ (2021) Information technology for healthcare managers (9th Edition) Health Administration Press: Chicago.](https://www.amazon.com/Information-Technology-Healthcare-Managers-Ninth/dp/1640551913)
23. [Tan J (2021) Adaptive health management information systems: Concepts, cases, and practical applications (4th Edition). Jones & Bartlett Learning. Burlington, MA.](https://www.jblearning.com/catalog/productdetails/9781284153897)
24. [Carter RA (2020) Dealing with data: Cybersecurity in the Covid-19 era. E&MJ, August.](https://www.e-mj.com/features/dealing-with-data-cybersecurity-in-the-covid-19-era/)