Advances in Radiation Oncology (2022) 000, 100897

advances
in radiation oncology

www.advancesradonc.org

Clinical Investigation

Impact of and Response to Cyberattacks in Radiation Oncology

Carl J. Nelson, MD,* Emilie T. Soisson, PhD, Puyao C. Li, MD, Nataniel H. Lester-Coll, MD, Havaleh Gagne, MD, Matthew A. Deeley, PhD, Christopher J. Anker, MD, Lori Ann Roy, MHA, and H. James Wallace, MD

Division of Radiation Oncology, University of Vermont Larner College of Medicine, Burlington, Vermont

Received October 19, 2021; accepted December 16, 2021

Abstract

Cyberattacks on health care facilities are increasing and significantly affecting health care delivery throughout the world. The recent cyberattack on our hospital-based radiation facility exposed vulnerabilities of radiation oncology systems and highlighted the dependence of radiation treatment on integrated and complex radiation planning, delivery and verification systems. After the cyberattack on our health care facility, radiation oncology staff reconstructed patient information, schedules, and radiation plans from existing paper records and physicians developed a system to triage patients requiring immediate transfer of radiation treatment to nearby facilities. Medical physics and hospital information technology collaborated to restore services without access to the system backup or network connectivity. Ultimately, radiation treatments resumed incrementally as systems were restored and rebuilt. The experiences and lessons learned from this response were reviewed. The successes and shortcomings were incorporated into recommendations to provide guidance to other radiation facilities in preparation for a possible cyberattack. Our response and recommendations are intended to serve as a starting point to assist other facilities in cybersecurity preparedness planning. Because there is no one-size-fits-all response, each department should determine its specific vulnerabilities, risks, and available resources to create an individualized plan.

Introduction

On October 28, 2020, a joint alert was issued by the U. S. Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the U.S. Department of Health and Human Services warning of “credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers.”[1] At approximately 11 AM that day, the University of Vermont Health Network (UVMHN) experienced multiple clinical system outages as a result of a cyberattack. Access to the internet, hospital servers, and remaining clinical systems was immediately halted by our information technology (IT) infrastructure team to minimize further propagation of malware. As a result, all hospital electronic medical records (EMR), laboratory, pharmacy, pathology, radiology, and hospital phone and email systems were inaccessible.

Immediate Effects

The complete and immediate shutdown of UVMHN information and communication systems had an overwhelming impact on patients and providers. After months

Sources of support: This work had no specific funding.

Disclosures: none.

Data sharing statement: Research data are stored in an institutional repository and will be shared uponrequest to the corresponding author.

*Corresponding author.; E-mail: carl.nelson2@uvmhealth.org

https://doi.org/10.1016/j.adro.2022.100897

of COVID-19 restrictions that limited staff interactions, hospital staff had adapted to physical distancing restrictions by implementing remote staffing plans and telemedicine visits that were dependent on offsite access to hospital information systems.

By noon of the first day of the cyberattack, the radiation oncology information system (ROIS) (Elekta MOSAIQ) required for radiation treatments and scheduling became inaccessible and all remaining radiation treatments were canceled. Further assessment of system outages in radiation oncology revealed the loss of phone and email capability and inoperability of the hospital EMR system. However, the radiation treatment planning system (TPS) residing on a UNIX server (Philips Pinnacle) was unaffected by the system outages and remained operational, including the ability to export digital imaging and communications in medicine (DICOM) data to local drives. Despite the fact that the hospital picture archiving and communication system was down and images taken in radiology could not be accessed, the computed tomography simulator remained functional and direct transfer of DICOM images to the TPS was restored quickly.

Because patient information was inaccessible, no contact information was available to inform patients of treatment cancellations. Patients arriving for canceled radiation treatments were asked for their contact information and this was recorded on paper. With no access to electronic patient information, treatment schedules, or current radiation dose, the radiation oncology team compiled a physical chart for each patient using previously printed demographics and schedules. Using printed patient information, the radiation therapists, nurses, administrative staff, and physicians started daily phone calls to patients to keep them updated on the evolving situation. As the community learned of the cyberattack, patients were understandably distressed by their treatment interruption, but also sympathetic and understanding of the circumstances.

Triage and Clinical Effects During Early Stages of Cyberattack

After the loss of the ROIS on the first day of the cyberattack, the established departmental contingency plan was to restore the most recent backup files to the ROIS. However, after IT security shut down all servers, no access to the ROIS or backup files was permitted until the servers were scanned and cleaned of any security threat. With an estimated wait time of 2 to 3 weeks before we could gain access to the ROIS or the backup database, medical physics and IT determined that a new ROIS needed to be built in a standalone server in radiation oncology.

As it became clear that resumption of network services could take multiple days, if not weeks, it was imperative to find safe, alternative treatment system solutions that did not rely on network connectivity to minimize radiation treatment breaks for our patients. It was also clear that these solutions would not be immediately available to all patients, so physicians needed to develop a framework to prioritize patient treatments. These efforts were made more challenging by hospital-wide COVID-19 restrictions for physical distancing, which limited in-person meetings to no more than 6 people. The new IT-imposed restrictions shut down internet and hospital WiFi, which eliminated access to secure email, video, or telecommunications. With our main methods of information exchange via hospital EMR, email, and video conferencing unavailable, providers and staff had to rely on personal messaging services and small group meetings for communication and planning.

Because extended treatment breaks had the potential to affect the oncological outcomes for some patients more than others, the physicians prioritized patient treatments while striving to maintain an ethical and practical framework for these treatment decisions based on treatment intent, tumor biology, and anticipated effect of treatment delays.[2-6] Patients were individually triaged by physicians and stratified into groupings for treatment. Triage group 1, requiring the most immediate need to resume treatment, included patients already undergoing curative treatment with primary radiation or concurrent chemotherapy and radiation. The second triage group included patients approaching the end of their radiation course. Triage group 3 consisted of patients with tumors expected to have slower cell repopulation, such as prostate cancer or low- risk breast cancer.[7]

After the attack, the treatment options immediately available included transferring patients to our affiliated sites or treating onsite with manual operation of the linear accelerator (LINAC) outside of the ROIS. Both solutions came with potential risks and patient effects, which required rapid development of safety procedures to mitigate risks. Transferring patients to other sites presented significant logistical challenges, while there were ethical considerations to keeping patients onsite and treating in a limited capacity. Fortunately, the DICOM images, structures, and plan information remained accessible despite the loss of the ROIS and could be exported to local drives and physically transported to other sites for replanning.

Although multiple options were explored for transferring patients to outside facilities, and most regional cancer centers offered assistance, the most practical option was to transfer patients to an affiliated UVMHN site based on geographic proximity. The UVMHN radiation oncology practice consists of a main clinic at UVM Medical Center (UVMMC) and 2 affiliated clinics. The affiliated facilities initially had system disruption on the first day of the cyberattack, but the majority of the clinical systems were restored the following day, and radiation treatments resumed for their patients. The UVMMC patients in triage group 1 were offered treatment at the affiliated radiation facilities. The closest affiliated radiation facility is a 45-minute drive from the main campus, and an initial cohort of 11 patients accepted this offer and resumed radiation within 1 week of the cyberattack. A team of 3 dosimetrists replanned these cases for treatment at the affiliate site using saved DICOM images and structure sets from the operational TPS at the main site. Immobilization equipment was transferred to the affiliated clinic and a therapist from the main clinic was reassigned to the affiliated clinic to ensure continuity of care and to provide additional working knowledge of setup and other patient-specific variables. Physicians from the main clinic also traveled to the affiliated clinic at the beginning of treatment to aid in the transition.

Physics, Operations, and Safety Concerns

Due to the limited capacity of the affiliate site and the logistical challenges for many patients involved with traveling to other centers for treatment, it was not possible to transfer all patients outside the main UVMMC site, and the remaining patients required on-site treatment options. The only immediately available option required treating patients with manual operation of the LINACs. For Elekta LINACs, manual operation can only occur in service mode. In non-emergency situations, treating outside the ROIS would not be considered. However, after an analysis of the potential risk for errors in manual operation of the LINAC compared with the risks of prolonged treatment breaks, it was decided that this method was an acceptable emergency option for select patients. Treatment could only proceed manually using 1 of 2 methods. In the first method, beams could be created manually by entering each beam parameter. In the second method, DICOM information could be imported to the LINAC and the treatment field would be created directly from the exported plan information.

Medical physics developed in-house code to parse and transform DICOM data from the TPS to allow for direct import of data into the LINAC. However, for safety concerns it was decided to reserve this technique as a last resort, and it was never used.[8] Although manual beam delivery is routinely used for physics testing, there were safety concerns with clinical treatment of patients without ROIS connectivity. The first consideration was that treatment outside the ROIS bypasses multiple safety checks offered by automatic record and verify systems. For example, this method of treatment delivery did not record the number of fractions or total dose delivered to the patient and there was no method to account for beam interruptions during treatment and other recovery mechanisms. The second consideration was that the LINAC coordinate system differed from the coordinate system in the treatment plans. As a result, all beams were entered manually and had to be converted from plan coordinates to machine coordinates before entry. Although this conversion was not complex, it did present an additional opportunity for errors and required an associated mitigation strategy. Finally, while DICOM information technically can be brought into the LINAC directly to allow for treatment of complex intensity modulated radiation therapy fields, it was not without significant challenges and patient risks. Only manually entered rectangular fields and electron applicators that could be easily verified were considered a safe treatment option. Because the high priority patients with complex plans did have other options that were felt to be safer, manual treatments were limited to simple fields that could be easily verified.

Before moving forward with manual treatments, specific safety rules and quality checklists were established. First, all data were entered manually into the LINAC by physicists familiar with manual beam delivery and then checked by a second physicist. Second, a policy was established that physicists were present at the machine for each manual treatment and a paper copy of all beam information was created to check against the machine parameters.

Because simple electron fields were determined to be safe to deliver manually, the first set of patients to be treated in manual mode were electron boost fields. This allowed patients undergoing radiation for breast cancer to resume electron breast boost treatments, while the remaining patients with breast cancer had their electron boosts started early to minimize gaps in treatment. Implementation of this immediate response allowed 17 patients with breast cancer to resume treatment using an electron boost with only a 2-to-3 day break. Several patients also received treatment with simple 3-dimensional plans using manual mode, and 1 patient was able to undergo single fraction palliative spine radiation using this method. Ultimately, no complex plans were treated outside the ROIS and high priority was given to rebuilding the ROIS to avoid that scenario. As the IT team and the equipment vendor worked 7 days a week to rebuild the ROIS with a standalone “downtime” server, patients were either transferred, on break, or treated manually depending on clinical need and plan complexity (Table 1).

Limited Resumption of Hospital and Oncology Services

As the network downtime continued into a second week, the backlog of patients requiring simulation and treatment started to grow, as did referrals for new patient consultations and emergency radiation treatment for inpatients. Because there was no access to patient records in the hospital EMR or ROIS during the first weeks of the cyberattack, clinic visits were rescheduled until pathology

Table 1 Approaches to addressing interruption of care owing to cyberattack

	Number of patients
Moved treatment to satellite location	17
Added fraction	3
Weekend treatments	47
Switched to boost early (electrons, service mode)	17

and imaging could be accessed. Eventually, providers gained access to a statewide database, Vermont Information Technology Leaders, which allowed read-only access to contact and clinical information from all enrolled providers in the state. Although the information available was limited, it did allow for resumption of a significant amount of care within 1 to 2 weeks of the attack.[9]

Throughout this initial downtime the computed tomography simulator and the TPS remained operational. However, because there was no certainty regarding when patients could be treated with anything other than electrons or simple treatment plans, new patients were triaged and treatment postponed for those not requiring immediate treatment. Similar to the initial triage groupings developed for patients on treatment, new patients determined to be at low-risk if their treatment was delayed included those with benign tumors, patients with prostate cancer undergoing androgen deprivation, elderly low-risk patients with breast cancer who could be treated with hormone therapy and patients with early stage, indolent non-small cell lung cancer who were under consideration for stereotactic body radiation therapy.[10] Patients requiring curative intent primary radiation therapy were prioritized, along with patients who had undergone surgery and patients for whom timely initiation of radiation was associated with improved survival.

Through extraordinary cooperation and diligence, the UVMMC IT team, the ROIS vendor, and the medical physics staff built the new ROIS server and configured the treatment LINACs and full treatment resumed in less than 2 weeks. Staff worked long hours to repopulate patient data and treatment plans into the new ROIS database and complete all required quality and safety checks (Fig 1). As radiation treatment resumed using the new ROIS "downtime" server, each physician, in consultation with peers, developed a remediation strategy to deal with the delays in treatment. Strategies included modification of schedules to treat some patients with 6 radiation fractions per week to shorten overall treatment time, while others were prescribed an additional fraction to compensate for treatment breaks of 5 days or greater.

However, although services and treatment were restored in radiation oncology, other departments in the hospital struggled with compromised systems and many aspects of patient care remained limited. The radiology picture archiving and communication system was inaccessible and radiology limited studies to emergency imaging for inpatients. Scheduled radiology examinations for cancer screening, staging, and surveillance were canceled and a growing backlog developed. A radiology and oncology command center was created to manage imaging requests and identify regional hospital radiology resources patients could be referred to for required imaging. The command center included clinical and operations representatives from radiology departments at all regional medical centers and quickly established a dashboard of radiology accessibility that was updated daily. This dashboard allowed clinicians and nurse navigators to rapidly triage and refer patients to regional centers for imaging. Hospital system outages for laboratory services and chemotherapy infusion records were not readily accessible, and chemotherapy infusion patients were unable to receive intended oncology care.[11] Due to these delays and the need to divert patients to other cancer centers, chemotherapy infusion visit volume dropped by 52% initially and then incrementally increased as services slowly recovered over the following month.[12]

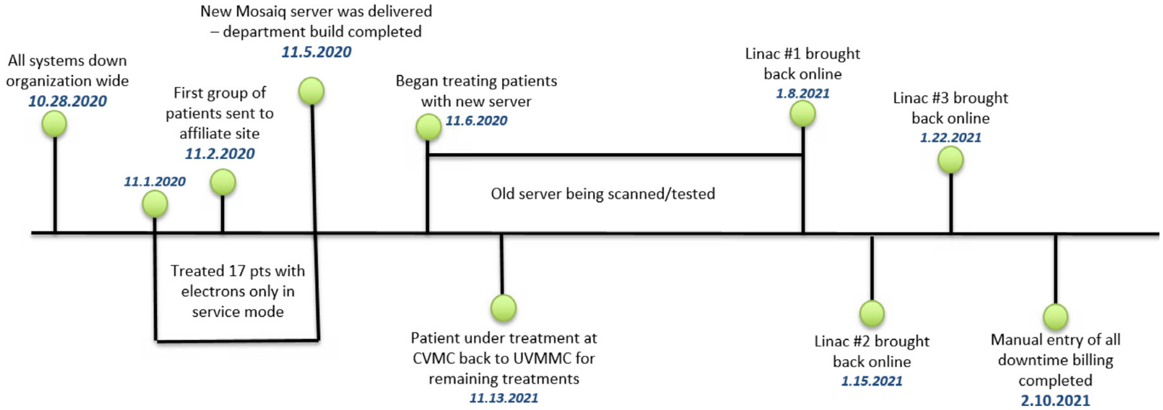
All systems down organization wide
10.28.2020
11.1.2020
First group of patients sent to affiliate site
11.2.2020
New Mosaiq server was delivered – department build completed
11.5.2020
Began treating patients with new server
11.6.2020
Old server being scanned/tested
Linac #1 brought back online
1.8.2021
Linac #3 brought back online
1.22.2021
Treated 17 pts with electrons only in service mode
Patient under treatment at CVMC back to UVMMC for remaining treatments
11.13.2021
Linac #2 brought back online
1.15.2021
Manual entry of all downtime billing completed
2.10.2021

Fig. 1 Timeline of cyberattack and radiation oncology response.

Discussion

There were multiple factors intrinsic to the radiation oncology structure at UVMMC that led to a successful response to the cyberattack. First, the TPS remained accessible throughout the cyberattack, as it resided on local servers that were not affected by the attack. Additionally, the UVM-affiliated radiation oncology site used the same TPS and had established shared resources with UVMMC, including physicists, dosimetrists, and physicians. This facilitated the rapid transfer of radiation therapy plans from our main site to the affiliated site for high-priority patients for whom prolonged interruption of treatment could have resulted in compromised cancer outcomes. Within this integrated system, UVMMC dosimetrists and medical physicists helped reconstruct radiation treatment plans for patients transferring care to the affiliated site to ensure consistent quality. Although the LINACs at each site were from different machine manufacturers, the affiliate site dosimetrist was key in identifying subtle differences in approaches to planning that made the process more efficient. The transfer of patient treatment also benefited from the exchange of radiation therapists, physicists, and treating physicians from the main UVMMC site to the affiliated site to initiate treatment and ensure a smooth transition of care.

Standard practices of our administrative, nursing, and therapy staff also aided in the capture of important scheduling information. Treatment schedules were printed out daily for each LINAC and patients provided a printout of their personal treatment schedules, and these were collected after loss of the ROIS and reviewed by therapists and providers to calculate dose delivered and dose remaining.

Given the competing interests for IT support across the network, a major success was the strong advocacy from radiation oncology leadership to prioritize and reestablish radiation oncology services in the hospital. After the cyberattack, a network response command center was formed to facilitate communication and to develop a system-wide IT response. Based on ongoing concerns about additional attacks, these meetings were held in a secure fashion by phone on a daily basis until after the network had regained the majority of its services. Broad priorities for timing of reestablishing services were developed using a traditional triage model informed by input from clinical and operational leadership as well as medical ethicists. Patients undergoing potentially lifesaving therapies whose outcomes could demonstrably be affected by delays in treatment (including patients with cancer receiving radiation therapy) were among the highest priority. Therefore, significant IT resources were directed to develop a radiation oncology strategy and were invaluable to reestablish treatments as quickly as possible.

Shortcomings in Response

Despite the successful reestablishment of radiation treatment at UVMMC, our response to the cyberattack was limited by several factors. Because IT security took hospital network servers offline while computers were reimaged to ensure no malware remained on the network, the ROIS system backup data could not be accessed. As this backup planning was a major component of our departmental disaster response, loss of this patient treatment data limited the options for resuming treatment while IT and the activated Vermont National Guard scanned more than 5000 network computers.[13]

Although all efforts were made to determine the correct number of treatments before the cyberattack and document all treatments in downtime, the loss of the ROIS did result in errors. Despite vigorous measures including confirming treatment dates with each patient, we determined that 3 patients had 1 more treatment than initially planned. However, this small number of events is a testament to the risk mitigation strategies designed to ensure the safe treatment of patients. In each instance, the patient was notified of this event by the treating physician and the potential risk determined to be minimal.

As this attack occurred during the COVID-19 pandemic, many workplace restrictions remained in place that limited gathering of radiation oncology staff. The department was limited to small in-person meetings and the hospital had no effective means of rapidly disseminating information to coordinate care during the downtime. Similarly, COVID-19 restrictions prevented the ROIS vendor staff located outside of Vermont to physically travel to our site to help rebuild a server to host the new ROIS.

The impact of the cyberattack on patient care was overwhelming. Many patients requiring emergency care needed to be diverted to other hospitals, and the screening, diagnosis, and treatment for multiple medical conditions were delayed. With the loss of ability to provide many health care services, and the cost to restore the IT infrastructure, the financial effect of the cyberattack to UVMMC was estimated to cost the hospital between $40 million and $50 million,[14] with $1.5 million a day in lost revenue and recovery costs.[15] The financial impact on radiation oncology was an estimated loss of approximately $1.66 million in technical and professional payments.

Cyberattack Preparedness Moving Forward

The October 2020 cyberattack at UVMHN and other recent cyberattacks across the country exposed vulnerabilities in health care in general, as well as vulnerabilities specific to radiation oncology. Radiation treatment delivery is highly time sensitive and reliant on the connectivity of complex technology. Daily treatment delivery requires flawlessly working hardware and software integrated with systems throughout the hospital. Without EMR systems and with limited communication to coordinate with multidisciplinary teams, it is difficult to make treatment decisions. Furthermore, without a TPS, complex radiation treatment plans cannot be created or optimized. Finally, without a functioning record and verify ROIS system, planned treatments cannot be delivered.

Given the interconnectedness of hospital systems, implementing any technological solution to the challenges we faced required significant IT department involvement and support. In our case the cyberattack was only the beginning, and many of the limitations in accessing key technology were related to the later hospital-wide response to the attack. The response involved a cyber-forensics investigation with the Federal Bureau of Investigation and outside consultants and required careful restoration of systems with simultaneous implementation of stronger security measures.

Because our ROIS server resided within the hospital network and was not a cloud-based system, we were forced to build a new ROIS server. This ultimately required considerable time and effort to merge data from the temporary system back with our original system at a later date to maintain a complete system of all treatment records. An alternative consideration would be a cloud-based system that could provide potential advantages such as a quicker restoration of operations and a more seamless return to normalcy. However, the downside of a cloud-based system is that there may be more points of entry for a cyberattack and any related effect may be more widespread and simultaneous. This proved to be the case in a recent attack on a cloud-based ROIS services provider, which highlights the differences between a cyberattack involving a cloud based versus non−cloud-based record and verify system.[16]

Cyberattacks on health care and other vital industries are becoming more common.[17-19] In a previous publication and in the previous sections of this article, we discussed specific challenges we faced and unique solutions we implemented to quickly and safely resume treating patients.[20]

The lessons learned from this experience prompted us to further develop suggested practices for a radiation oncology department to prepare for, and be more responsive to, any future cyberattacks (Table 2).

Table 2 Suggested radiation oncology cybersecurity practices

1. Develop purposeful redundancies in software and/or hardware
Save frequent system backups stored offline that can be used to quickly restore function
Establish system “siloes” for key functionality and data, which would be exempt from hospital network shutdowns
2. Retain printed copies or offline and offsite backup of key records required for continuity of treatment
Departmental upcoming clinical schedule
Individual patient schedules
Patient contact information
Plan for destruction of printed patient records after predetermined period
3. Establish outage policies and procedures
Develop procedures for communication with staff and patients for when hospital-supported systems are down
Establish treatment priority for patients based on cancer type/stage and treatment intent
4. Establish a strong working relationship with the information technology department, as an actionable preparedness plan must incorporate their input, support, and prioritization
5. Perform disaster readiness exercises annually to test the strengths and weaknesses of departmental backup and contingency planning

An important caveat to our suggestions is that each cyberattack and hospital setting is different. Different hospitals and departments may have unique vulnerabilities based on available technologies and the effect of any attack. Therefore, there is no one-size-fits-all preparedness plan or solution. Ultimately, each department will need to determine its specific vulnerabilities, risks, and available resources to create an individualized preparedness plan for restoring patient care.[21,22]

References

1. Cybersecurity and Infrastructure Security Agency. Ransomware activity targeting the healthcare and public health sector. Available at: https://us-cert.cisa.gov/ncas/current-activity/2020/10/28/ransomware-activity-targeting-healthcare-and-public-health-sector. Accessed September 2020.
2. Shaikh T, Handorf EA, Murphy CT, Mehra R, Ridge JA, Galloway TJ. The impact of radiation treatment time on survival in patients with head and neck cancer. *Int J Radiat Oncol Biol Phys*. 2016;96:967–975.
3. Raphael MJ, Ko G, Booth CM, et al. Factors associated with chemoradiation therapy interruption and noncompletion among patients with squamous cell anal carcinoma. *JAMA Oncol*. 2020;6:881–887.
4. Fyles A, Keane TJ, Barton M, Simm J. The effect of treatment duration in the local control of cervix cancer. *Radiother Oncol*. 1992;25:273–279.
5. Fortin A, Bairati I, Albert M, Moore L, Allard J, Couture C. Effect of treatment delay on outcome of patients with early-stage head-and-neck carcinoma receiving radical radiotherapy. *Int J Radiat Oncol Biol Phys*. 2002;52:929–936.

6. Withers HR, Taylor JMG, Maciejewski B. The hazard of accelerated tumor clonogen repopulation during radiotherapy. *Acta Oncol*. 1988;27:131–146.
7. Gay HA, Santiago R, Gil B, et al. Lessons learned from Hurricane Maria in Puerto Rico: Practical measures to mitigate the impact of a catastrophic natural disaster on radiation oncology patients. *Prac Radiat Oncol*. 2019;9:305–321.
8. Pinkham DW, Sala IM, Soisson ET, Wang B, Deeley MA. Are you ready for a cyberattack? *J Appl Clin Med Phys*. 2021;22:4–7.
9. VITL. VITLAccess clinical portal. Available at: https://www.vitl.net/connect/provider-services/vitlaccess. Accessed September 2021.
10. No H, Lester-Coll N, Seward D, et al. Active surveillance for medically inoperable stage IA lung cancer in the elderly. *Cureus*. 2018;10:e3472.
11. Barry E. Patients of a Vermont hospital are left ‘in the dark’ after a cyberattack. Available at: https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html. Accessed September 2021.
12. Ades S, Herrera DA, Lahey T, et al. Cancer care in the wake of a cyberattack: How to prepare and what to expect. *JCO Oncol Pract*. 2021 OP2100116.
13. Jickling K. National Guard cybersecurity team deployed after UVM Medical Center hack. VTDigger. Available at: https://vtdigger.org/2020/11/04/national-guard-cybersecurity-team-deployed-after-uvm-medical-center-hack/. Accessed September 2021.
14. Benninghoff G. Malware on employee’s company computer led to cyber attack on UVM Medical Center. VTDigger. Available at: https://vtdigger.org/2021/07/21/malware-on-employees-company-computer-led-to-cyber-attack-on-uvm-medical-center/. Accessed September 2021.
15. Associated Press. Vermont hospital cyberattack cost estimated at $1.5M a day. Available at: https://www.securityweek.com/vermont-hospital-cyberattack-cost-estimated-15m-day. Accessed September 2021.
16. HIPAA Journal. Radiation treatments disrupted after cyberattack on software vendor. Available at: https://www.hipaajournal.com/healthcare-providers-postpone-radiation-treatments-cyberattack-elekta. Accessed September 2021.
17. Hoffman M. Nearly 2 weeks in, Scripps Health still fighting disruptive cyberattack. Available at: https://www.kpbs.org/news/2021/may/13/ongoing-scripps-cyber-attack-nears-two-weeks-uncle. Accessed September 2021.
18. Perlroth N. Irish hospitals are latest to be hit by ransomware attacks. Available at: https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html. Accessed September 2021.
19. Joyce C, Roman FL, Miller B, Jeffries J, Miller RC. Emerging cybersecurity threats in radiation oncology. *Adv Radiat Oncol*. 2021;6:100796.
20. Zhang B, Chen S, Nichols E, D’Souza W, Prado K, Yi B. A practical cyberattack contingency plan for radiation oncology. *J Appl Clin Med Phys*. 2020;21:181–186.
21. Nelson C, Lester-Coll N, Li P, et al. Development of rapid response plan for radiation oncology in response to cyberattack. *Adv Radiat Oncol*. 2020;6: 100613.
22. Harrison AS, Sullivan P, Kubli A, et al. How to respond to a ransomware attack? One radiation oncology department's response to a cyber-attack on their record and verify system. *Pract Radiat Oncol*. 2021. S1879-8500(21)00275-7.