SA–CME Information

THE IMPACT OF CYBERSECURITY IN RADIATION ONCOLOGY: LOGISTICS AND CHALLENGES

Description
Breaches in cybersecurity can levy drastic consequences in radiation treatment delivery and health care overall. This review article describes experiences and unique needs and strategies pertaining to radiation oncology IT infrastructure, electronic medical records, automatic time outs, treatment planning and delivery, plan verification, screen locking and more to help prevent and overcome a cyber disaster.

Learning Objectives
After completing this activity, participants will be able to:
1. Recognize critical areas of cybersecurity risk in the radiation oncology department/clinic.
2. Adopt strategies to bolster cybersecurity within the radiation oncology department.

Authors
Elizabeth M. Nichols, MD, is assistant professor and clinical director, **Shafiq Ur Rahman, MBA, MS**, is director of radiation oncology IT, and **Byongyong Yi, PhD**, is a professor, University of Maryland School of Medicine, Department of Radiation Oncology.

OBTAINING CREDITS

Instructions: To successfully earn credit, participants must complete the activity during the valid credit period.
To receive SA–CME credit, you must:
1. Review this article in its entirety.
2. Visit www.appliedradiology.org/SAM.
3. Login to your account or (new users) create an account.
4. Complete the post test and review the discussion and references.
5. Complete the evaluation.
6. Print your certificate.

Date of release and review: December 1, 2018
Expiration date: November 30, 2020
Estimated time for completion: 1 hour

Disclosures: No authors, faculty, or individuals at the Institute for Advanced Medical Education (IAME) or *Applied Radiation Oncology* who had control over the content of this program have relationships with commercial supporters.

Accreditation/Designation Statement: The IAME is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. The IAME designates this journal-based activity for a maximum of 1 AMA PRA Category 1 Credit™. Physicians should only claim credit commensurate with the extent of their participation in the activity. These credits qualify as SA-CME credits for ABR diplomates, based on the criteria of the American Board of Radiology.

Commercial Support: None

As part of this CME activity, the reader should reflect on how it will impact his or her personal practice and discuss its content with colleagues.

SA-CME (see page 13)

The impact of cybersecurity in radiation oncology: Logistics and challenges

Elizabeth M. Nichols, MD; Shafiq Ur Rahman, MBA, MS; Byongyong Yi, PhD

In May 2016, a large metropolitan health care organization consisting of 10 hospitals and numerous outpatient facilities was subject to a ransomware attack.[1] When employees logged onto their workstations, a pop-up message demanded a payment of 45 bitcoin (roughly $19,000) to unlock patient-related data (access to electronic medical records [EMRs]). In response, all computer systems/networks and interfaces of health system "X" were shut down, including those at a radiation oncology facility. It took several days for the health care organization to regain full functionality, including the radiation oncology practice (herein called XRO).

Dr. Nichols *is assistant professor and clinical director,* ***Mr. Rahman*** *is director of radiation oncology IT, and* ***Dr. Yi*** *is a professor, University of Maryland School of Medicine, Department of Radiation Oncology.* *Disclosure: The authors have no conflicts of interest to disclose. None of the authors received outside funding for the production of this original manuscript and no part of this article has been previously published elsewhere.*

XRO had to cancel 36 treatment appointments on day 1 of the attack as well as all appointments on days 2 and 3 post-attack. On day 3 post-attack, XRO began to contact another local major health care system with an established radiation oncology practice (herein YRO) to discuss the potential of patient transfers for continuation of treatment as the radiation oncologists felt that the unintentional break coupled with the unknown time of when the network would return would be potentially detrimental to patient outcomes. YRO and XRO were subsequently tasked with how to make this transition possible without access to the record and verify system, the tried and true record of radiation delivery. As these discussions took place, the XRO computer network was restored on day 4 post-attack and patient transfers were not required. While this scenario may seem like "something that could never happen to me," any radiation oncologist or practice could experience it at any time, especially those in metropolitan areas.

A 2014 study by Filkins et al showed that 94% of health care institutions have been victims of cyberattacks.[2] Of attacks aimed at the health care industry, 72% were directed against hospitals, clinics, large group practices and individual providers, while 28% of malware attacks were directed at provider organizations, health plans, pharmaceutical companies and other health care entities.[3] Health-related cyberattacks are generally categorized into four groups: data loss, monetary theft, attacks on medical devices and infrastructure attacks.[4]

As a result of increased health-related cyberattacks, the FDA issued a safety communication in June 2013 titled, "Cybersecruity for Medical Devices and Hospital Networks," which called for greater private-sector involvement and the establishment of a risk-based regulatory framework. Unfortunately, the guideline lacked specific details or regulations on how

SA-CME (see page 13)

healthcare networks could accomplish these goals.[5] The Ponemon study suggested, however, that networks focusing on cybersecurity with a specific recommendation to hire and empower a chief information security officer and establish incident response capabilities can reduce potential cybersecurity risks by 42%.[6] Cybersecurity is a major focus of health care as a result of these staggering statistics, and the FDA has ongoing efforts focused on cybersecurity and public health, including public workshops (www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm).

In this article, we will discuss logistics of cybersecurity particularly as they pertain to radiation oncology, as well as resultant challenges. We also will describe how our organization has navigated some of these logistics and challenges, as this may prove helpful to other organizations.

Challenges of Cybersecurity in Radiation Oncology

The healthcare industry has been the target of increasing cyberattacks over the last several decades. The complexity of the healthcare industry as well as laws surrounding patient privacy make cybersecurity a top priority resulting in extensive and robust hospital IT departments. Similar to radiology, radiation oncology has specific software required to utilize and operate machinery/departments. This requires unique IT expertise to assist users, troubleshoot problems and manage/store large amounts of data. For sites where radiation oncology has its own IT group, it is critical to define roles and responsibilities, workflows, and monitoring systems to align with hospital-based policies and procedures.

Radiation Oncology IT Infrastructure

Some of the general topics required for a successful radiation oncology IT group (or integration into the hospital IT system) are to organize, develop, document and disseminate personnel roles and define access to control policies. Much like hospital-based EMRs, "super-users" or "builders" must be defined and limited to ensure data quality. Policies and procedures must be developed in accordance with hospital-based policies and also revised at regular intervals. For example, if the hospital-based EMR has a time-out policy of 10 minutes, radiation oncology software should follow the same policy. Hospital IT departments typically have clear procedures for monitoring/auditing of the EMR by monitoring system accounts and user access to ensure patient privacy. They also have procedures for granting and revoking access around employee hires, terminations, etc. It is critical that radiation oncology IT follows similar procedures as these are often not controlled by the hospital-based IT group.

Radiation oncology IT must collaborate with multiple EMR systems with several teams in managing the appropriate functioning of these applications (hospital, machine vendor, treatment planning system [TPS] vendor, etc.). There are also significant challenges with interfaces from radiation oncology technology to hospital systems in part because hospital IT departments generally lack knowledge regarding radiation oncology workflows and technological needs, which can make interface development and maintenance difficult.

Radiation oncology is a research-oriented field with increasing demands from institutional research bodies as well as national research governing bodies such as the NRG. For example, many patients enrolled in NRG trials need to have DICOM information as well as numerous demographic and cancer characteristics sent to centralized databases. Developing safe, efficient workflows around these processes is quite challenging.

Lastly, there is also a need to monitor and maintain these systems with routine upgrades. These require significant work efforts in conjunction with vendor support. Many future vendor upgrades focus specifically on cybersecurity.

Logistics of Cybersecurity in Radiation Oncology

Radiation oncology is undoubtedly one of the most technical fields in medicine both in terms of radiation technology as well as information technology infrastructure. Linear accelerators (linacs) require frequent maintenance and quality assurance with standard schedules. Several manufacturers have taken new approaches of remote access to fix technical issues and perform routine maintenance. Treatment areas/rooms are equipped with vendor-controlled networks behind their firewall for their certified configuration and security. Many hospital systems have firewalls in place to prevent this type of access as the concern is that malware from the manufacturer could potentially enter the hospital network through this type of access.

At our institution, this has been raised as a cybersecurity concern to the hospital environment and special permission had to be obtained from hospital leadership to allow vendor access. Our radiation oncology IT team designed a subnetwork for each treatment room in the hospital network that effectively separates each treatment room and vendor-controlled firewall with a hospital-managed firewall, allowing for secure transmission of data (two layers of firewalls). Both the vendor-supported and hospital-based firewalls have controlled access to allow for continuous treatments. This design ensures the radiation oncology treatment rooms are securely isolated from other sections of the hospital IT infrastructure in the event of malware.

In the past, many radiation oncology vendors also utilized USB disks for data transfers. USBs can pose a significant cybersecurity threat if left unencrypted/unsecure as malware attached

SA-CME (see page 13)

to the USB can be transferred between computers and systems. Vendors have made significant improvements to limit the need for USB transfers; however, this need has not been completely eliminated. Continuous product improvement is needed in this arena among vendors and clients to further minimize these risks. When a USB must be used it is critical that it is encrypted and secure.

Electronic Medical Records

Commercially available hospital EMRs cannot be the sole EMR system for radiation oncology practices due to their inability to operate linacs. As such, all radiation oncology practices require radiation oncology software such as ARIA (Varian, Palo Alto, California), MOSAIC (Elekta, Stockholm, Sweden), or others. Most hospital-based practices have been asked to integrate to the hospital EMR, posing significant challenges to the workflow and operations of radiation oncology practices, especially as most of these software programs have no integration with radiation oncology EMRs. Major vendors such as Varian and Elekta have now devoted specific resources to assist with this integration; however, much of this still depends on custom-built interfaces, which expose both systems to risk. Additionally, hospital systems must make decisions regarding uni- or bi-directional interfaces, each of which poses risks to the EMR systems.

More recently, Epic Systems Inc. (Verona, Wisconsin), developer of one of the most popular EMR systems used in the United States, says it is developing a module specific to radiation oncology. While this undoubtedly will not replace radiation oncology EMR systems, it will hopefully ease the burden on radiation oncology EMR integration.

Standard components of hospital-based EMR systems are hospital data governance, compliance audits and firewall testing, all of which support health system security. At this point, these features are not standard in radiation-oncology-based EMRs. For radiation oncology practices in which the EMR system is not governed by the hospital, it is critical to have the same level of auditing and testing to ensure appropriate cybersecurity.

Automatic Time Outs

One of the basic tenets of cybersecurity is automatic time outs and/or locking of computers both for reduced access/opportunity for malware/viruses as well as compliance with the Health Insurance Portability and Accountability Act (HIPAA). These pose unique challenges for some of the workflows in radiation oncology.

Treatment Delivery

Radiation therapists need to have several computer screens/operations functioning to treat patients safely. The treatment control system (TCS), EMR, and other secondary treatment systems (eg, BrainLab, AlignRT) all must open simultaneously for safe, quality patient treatment. As therapists are often in and out of rooms and sometimes attending to patients for > 5 to 10 minutes without attending to a computer screen, automatic time outs result in lost work and decreased efficiency. This inadvertently can increase treatment times, as every time a therapist must log into the computer and EMR system, roughly 30 to 90 seconds are lost. Multiplied across 20 treatment sessions in a day, it is equivalent to an entire treatment slot. As hospitals are focused on quality and efficiency, this can be viewed as an opportunity for lost revenue in terms of "one less patient treated" as well as potentially increased cost of therapy staff time.

Treatment Planning

Treatment planning and plan optimization algorithms take significant amounts of time. Plan optimization can require several hours depending on plan complexity and the radiation technique (such as proton therapy). In many cases, dosimetrists may set complex plan optimization to occur overnight to increase their workflow efficiency. However, automatic time outs prevent dosimetrists from doing this as in many cases the TPS closes once the time out is performed. In our proton center, for example, if a plan optimization does not start by the early afternoon, the dosimetrist must choose between working extremely late (while touching their computer every 30 minutes to prevent the time out) vs. waiting another day to start the optimization. Similar to therapy, this can cause significant workflow challenges.

Plan Verification

While plan verification systems have also become quicker and more efficient, the same issues can apply to the physics workflow as described above for treatment planning.

Locking Screens in Unattended Computer Systems

Another tenet of cybersecurity and HIPAA compliance in the EMR era is locking a computer screen when the computer is unattended, even for a moment. This requires the user to lock the screen; however, if the EMR is accessed for a particular patient record, then that record can remain "locked," preventing another from saving information in the record. This can result in many challenges for the radiation oncology workflow for all radiation oncology users. For example, two to three therapists work on a machine. If one therapist logs into the EMR and locks the screen but another therapist needs to document in the chart, this can cause save-back issues in which one individual's work can be lost. This is potentially common for the therapy group that is constantly in and out of rooms, and again, can significantly obstruct workflow.

Our Approach to Cybersecurity and IT

The University of Maryland Medical System is comprised of 13 hospitals

SA-CME (see page 13)

across the state along with numerous outpatient practices. As a general matter, all of the hospitals operate Epic EMRs, although as of press time, several hospitals were transitioning from their legacy system. The University of Maryland Radiation Oncology Department consists of six practices, three in system hospitals and three freestanding. One of these practices is a proton center. All practices use Varian linacs, and the proton center uses a Varian cyclotron. We use ARIA as our radiation oncology EMR, and both the Varian Eclipse and RayStation (RaySearch laboratories, Stockholm, Sweden) treatment planning systems.

All six locations use a single, central ARIA database and all linacs are commissioned to the same standard, which allows for ease of patient transfers between practice locations. The ARIA application was integrated to include all of our network sites several years ago, which has significantly lowered system-level operational costs.

Five of our six practices have interfaces built between Epic and ARIA, and one continues to operate the Meditech (Westwood, Massachusetts) system but will transition in the future. In our hospital system, Epic is considered the "source of truth." Our clinicians perform all clinical documentation except for on-treatment notes and end-of treatment notes in Epic. All orders (lab, medication, imaging) are also performed in Epic. On-treatment and end-of-treatment notes are initiated in ARIA and interfaced to Epic. This workflow was chosen to allow for the auto-population function of dose/fractionation provided by ARIA.

A critical component for interfacing is having the correct account number attached to the note. The hospital system allows only unidirectional interfaces and, as a result, many workarounds were created for patient workflow. For example, since patient treatment times and machines often fluctuate, patient treatment appointments are not interfaced to Epic. The downside is that our medical oncology colleagues cannot see the radiation oncology treatment schedule. Consult and follow-up visits are scheduled in Epic and interfaced to ARIA. A reconciliation process is performed every night to ensure all visits are interfaced. While working with Epic can initially be demanding, we have created workflows that minimize duplication of staff/faculty effort and have successfully reduced duplicative efforts by 70%.

Several additional medical software systems are integrated in our model. In the Epic EMR system, secure data transmission is through HL7 (in-bound interfaces are ADT [admissions, discharges and transfers] and SIU [scheduling information unsolicited]) into ARIA and MDM (medical document management), while the outbound interfaces to Epic are for MDM, DFT-UPC (detailed financial transactions-universal product code). In our workflows with Meditech and other systems, interfaces for imaging reports, labs, SIU, DFT and MDM are also present. Creating secure communication lines requires education in various software systems and analysis of how custom-built interfaces will work together without duplicating patient records.

Regarding data governance and compliance audits, our department has its own data governance group for ARIA modeled after the hospital-based one. New hospital policies and procedures are reviewed in real-time and appropriate modifications are made. For example, when our hospital changed to an 8-minute time-out policy, this was modified in ARIA. Our hospital system engages a third-party vendor who performs cybersecurity audits on an annual basis for departments using separate EMR software. All our practice locations are firewall protected and undergo periodic testing at the hospital-system level.

To address challenges discussed above, we have created unique groups with unique rights depending on group member workflows. For example, the dosimetry location is not accessible to the general public. As a result, we have recently disabled the time-out procedure for dosimetry due to the difficulties it causes with plan optimization, especially at our proton center where this is known to take hours. While this was a difficult decision, it was felt that since the area was not accessible to the public and if users "locked" their screens, plans could still run in a secure manner without significant risk of a malware attack. In the treatment control areas, however, since patients and their family members can often see the computers, we did not feel comfortable making these changes. As a result, therapists are subject to some inconveniences in workflows discussed above.

While we live in a hybrid environment with vendor-provided devices, radiation oncology IT is responsible for the supporting infrastructure and an antivirus environment. Vendors frequently have exceptions to their software capabilities, which can pose risks to our IT environment. For example, the Elekta GammaKnife has a very secure system that prevents transmission of data even within our own local area network (LAN) to another system (such as ARIA). As a result, the only way users can transfer data is through a USB disk, which has a much higher risk for hackers/viruses/malware. These exceptions can pose a large risk to our environment and extra precautions are taken in these scenarios.

In addition, we have designed our system in a redundant style, serving our applications from two physical locations (main data center and our disaster recovery [DR] location). Depending on each kind of a disaster/attack (critical, medium, low), we have developed our DR plans to ensure patients can receive treatment. Our system is redundant in terms of database delivery, image and file delivery as well as different technologies

SA-CME (see page 13)

involved to deliver applications, such as domain controllers (DCs), Citrix controllers, data collectors, etc. We are actively working on a concept of a separate DR plan in case of an attack similar to that described in the beginning of this paper.

In radiation oncology, we cannot eliminate the importance of QA protocols for our daily/every treatment. We are delivering all of our QA applications from a central location with the same redundancy level.

Another healthcare institute experienced a cyberattack, and within 90 seconds their 15000 servers were infected and rendered unusable. This was the result of a single user clicking a wrong link. This highlights the importance of education of users as one of the best and first lines of protection. All ARIA users attend a mandatory RadOnc IT annual inservice where we speak about technology and cybersecurity. We also send notices to staff as needs arise to educate them on ways to avoid cyber risks. These are often in addition to any hospital-based emails/notifications.

The focus of radiation oncology IT is to ensure our mission of safe patient care will remain aligned by considering sizing needs, infrastructure and function/workflows.

Conclusion

Radiation oncology is a unique specialty with unique needs regarding cybersecurity. In our experience, most of the radiation oncology software lags behind that of hospital-based EMRs in regard to cybersecurity features and, as a result, the onus is on the user to ensure that appropriate measures are taken for the safety of our patients and staff. Future upgrades are prepared to enhance cybersecurity features; however, we would encourage all radiation oncology practices to develop a "disaster strikes" plan on how to handle such situations.

References

1. McCarthy J. MedStar attack found to be ransomware, hackers demand Bitcoin. *HealthcareITNews*. https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin. Published April 4, 2016. Accessed November 19, 2018.
2. Filkins B. *Healthcare cyber threat report: widespread compromised detected, compliance nightmare on horizon*. SANS Institute. March 6, 2014.
3. Maron DF. A new cyber concern: hack attacks on medical devices. *Sci Am*. June 25, 2013.
4. Perakslis ED. Cybersecurity in health care. *NEJM*. 5014; 371(5):395-397.
5. U.S. Food and Drug Administration, Medical Devices. *Cybersecurity*. https://www.fda.gov/medical-devices/digitalhealth/ucm373213.htm. Last updated 10/31/18. Accessed November 19, 2018.
6. Ponemon Institute. 2013 *Cost of data breach study: global analysis*. May 28, 2013.