



**RO•ILS**<sup>®</sup>

RADIATION ONCOLOGY  
INCIDENT LEARNING SYSTEM

Sponsored by ASTRO and AAPM

CLARITY

**PSO**

A Patient Safety Organization

---

## RO-ILS CASE STUDY 08

### IT PERMISSIONS DISRUPT HDR DELIVERY

#### Introduction:


Hospitals are increasingly becoming targets from hackers, ransomware and cyber security threats. A joint cybersecurity advisory, coauthored by the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation and the Department of Health and Human Services, recently described the tactics, techniques and procedures used by cybercriminals against health care entities for financial gain.<sup>i</sup> The advisory described an increased and imminent threat to hospitals and healthcare providers and provided details on how the attacks are carried out. The document also offered tips and best practices for hospitals and health care providers when confronted with these assaults.

Additionally, the American Medical Association issued a report “Technology Considerations for the Rest of 2020” itemizing the risks and vulnerabilities to which hospitals and health care providers are susceptible.<sup>ii</sup> It also provides a list of questions that hospitals should ask IT vendors regarding network security. Hospitals and practices have needed to improve their ability to keep protected health information (PHI) secure and may often take swift action to protect PHI.

The possibility of disrupting or interrupting the clinical workflow for any field exists but is especially relevant to radiation oncology given its high dependence on network connectivity between technology-based equipment. The importance of accessing critical health information and maintaining standardized processes has also increased as the COVID-19 pandemic has increased the utilization of telemedicine.

#### Case Example:

While attempting to treat the first fraction of a high-dose-rate (HDR) brachytherapy case, a staff member could not upload the treatment file to the treatment delivery computer. The treatment delivery computer reported errors when it attempted to retrieve the file from the oncology information system (OIS). The staff member contacted IT and then restarted the services on the treatment delivery computer that are necessary to communicate with the OIS. These actions did not correct the issue. To limit further delay in the treatment of the patient, it was decided that a physicist would manually enter the treatment information in the treatment delivery computer and then have a second physicist check the treatment information prior to the first treatment.



After the completion of the treatment, the staff member reached out to IT to determine the cause of the interoperability issue. It was determined that the HDR computer lost its membership in the domain. This prevented the treatment delivery computer from authenticating the treatment file with the OIS database. The radiation oncology IT team worked with hospital IT to restore domain membership of the treatment delivery computer. Testing was done to ensure interoperability between the systems.

### **Contributing Factors:**

- Lack of communication between radiation oncology department and hospital IT teams.
- Lack of pre-treatment testing regarding communication between the treatment delivery computer and the OIS.
- Interoperability/computer permissions down.

### **Lessons Learned/Mitigation Strategies:**

1. Clear and concise communication and integration between the radiation oncology department and hospital IT teams is essential for the function of the radiation oncology department.<sup>iii</sup>
2. It is necessary to develop an alternative method, independent of network functionality, to transfer treatment files between information systems.<sup>iv</sup>

A variety of sometimes seemingly innocuous IT updates (e.g., changes to firewall rules, antivirus software, operating systems, storage location) can cause issues with software/network permissions. Additionally, often hospital IT departments may not appreciate the intricate network of radiation oncology systems and equipment required for basic function. Therefore, it is imperative that the hospital IT and radiation oncology teams work together and have open communication regarding hardware, software, domain membership, etc. Teams need to establish an ongoing relationship and educate one another proactively on their needs and expectations. Consider scheduling regular meetings between IT teams and knowledgeable liaison(s) from the radiation oncology clinical staff to ensure frequent interaction and updates. It is important to recognize treatment control computers as medical devices that should not be subject to routine changes (e.g., should not auto power down, should not be upgraded/patched, should not be removed from the domain) without first clearing and coordinating with the clinical team to obtain consent from the department. With the number of cybersecurity threats increasing, hospital IT policies and procedures may change quickly. It is critical that radiation oncology be aware of these changes as early as possible, ideally prior to going into effect, and assess any potential impact on clinical workflow as this directly affects the level of quality and safety in the department.

Manually entering treatment information into the treatment delivery computer is not optimal and can be prone to error.<sup>iv, v</sup> An alternative or backup method of enabling treatment file transfers should be implemented. Preparing and practicing for emergency situations if the network goes down (e.g., utilizing an encrypted USB) should be a routine part of QA process. Standardized processes can be disrupted for a variety of reasons and while the causes may vary, practices should plan for how to handle disruptive scenarios with the highest safety standards and lowest risk possible.

## References:

<sup>i</sup>Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Section. United States Cybersecurity and Infrastructure Security Agency website. Updated October 29, 2020. Accessed February 9, 2021. [https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A\\_Ransomware%20Activity Targeting the Healthcare and Public Health Sector.pdf](https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20Activity%20Targeting%20the%20Healthcare%20and%20Public%20Health%20Sector.pdf)

<sup>ii</sup>Technology Considerations for the Rest of 2020. American Medical Association website. 2020. Accessed February 9, 2021. <https://www.ama-assn.org/system/files/2020-10/ama-aha-technology-considerations.pdf>

<sup>iii</sup>Siochi RA, Balter P, Block CD, et al. Information technology resource management in radiation oncology. *J Appl Clin Med Phys* 2009;10(4):16-35.

<sup>iv</sup>Siochi RA, Balter P, Bloch CD, et al. A rapid communication from the AAPM Task Group 201: recommendations for the QA of external beam radiotherapy data transfer. AAPM TG 201: quality assurance of external beam radiotherapy data transfer. *J Appl Clin Med Phys* 2010;12(1):3479.

<sup>v</sup>Kubo HD, Glasgow GP, Pethel TD, et al. High-dose-rate brachytherapy treatment delivery: report of the AAPM Radiation Therapy Committee Task Group No. 59. *Med Phys*. 1998;25(4):375-403.