ONCODAILY MEDICAL JOURNAL

Article

# An Independent Read-Only Verification and Risk-Management System to Maintain Radiotherapy Safety During Oncology Information System Failure

**Authors:** • Abdelfattah Elnaggar • Essam Shaaban

**Affiliation:** 1) Lincolnshire Community and Hospitals NHS Group, Lincolnshire, UK
2) Information Systems Department, Beni Suef University, Beni Suef, Egypt

**Corresponding Author:** abdelfattah.elnaggar@nhs.net

**Published:** May 06, 2026

doi.org/10.69690/ODMJ-011-0526-7409

ONCODAILY MEDICAL JOURNAL

Article

# An Independent Read-Only Verification and Risk-Management System to Maintain Radiotherapy Safety During Oncology Information System Failure

**Authors:** • Abdelfattah Elnaggar • Essam Shaaban

**Affiliation:** 1) Lincolnshire Community and Hospitals NHS Group, Lincolnshire, UK
2) Information Systems Department, Beni Suef University, Beni Suef, Egypt

**Corresponding Author:** abdelfattah.elnaggar@nhs.net

**Published:** April 24, 2026

## ABSTRACT

Modern radiotherapy services rely heavily on Oncology Information Systems (OIS) for treatment planning, verification, and delivery. Failure of these systems, whether planned or unplanned, presents a significant risk to patient safety and treatment continuity. Recent cyberattacks and system outages have demonstrated the vulnerability of radiotherapy services to digital disruption.

This study describes the design and validation of the Automated Radiotherapy Continuity System (ARCS), an independent, vendor-neutral, read-only verification system developed to maintain safe radiotherapy delivery during OIS downtime. ARCS mirrors DICOM-RT data, independently verifies patient and machine metadata, enforces fractionation limits, and requires medical physics approval prior to use. Validation testing was performed using anonymized DICOM-RT datasets representative of Varian and Elekta workflows. Across 100 test plans, ARCS achieved a mirroring accuracy of 99%, with system failover occurring in under five minutes following simulated OIS failure. No unsafe irradiation sequences were observed. ARCS provides a practical and clinically safe approach to maintaining radiotherapy continuity during OIS downtime, reducing reliance on manual procedures and improving patient safety.

**Keywords:** radiotherapy, oncology information system, downtime, DICOM-RT, patient safety, verification, cyber resilience, risk management.

## INTRODUCTION

Multiple myeloma (MM) is a malignant plasma cell Radiotherapy delivery depends on the accurate coordination of digital systems responsible for patient information management, treatment planning, verification, and documentation. The Oncology Information System (OIS) functions as the central hub linking treatment planning systems (TPS), imaging devices, and linear accelerators. As radiotherapy workflows become increasingly digital, dependence on the OIS has intensified[1]. When an OIS becomes unavailable due to hardware failure, software malfunction, scheduled maintenance, or cyberattack, radiotherapy departments can lose access to approved treatment plans, prescription details, and fractionation history. In such situations, departments typically revert to manual downtime protocols involving the transfer of treatment data via external storage devices and manual reconstruction of treatment parameters. These processes are time-consuming, cognitively demanding, and vulnerable to error, particularly under

clinical pressure[2].

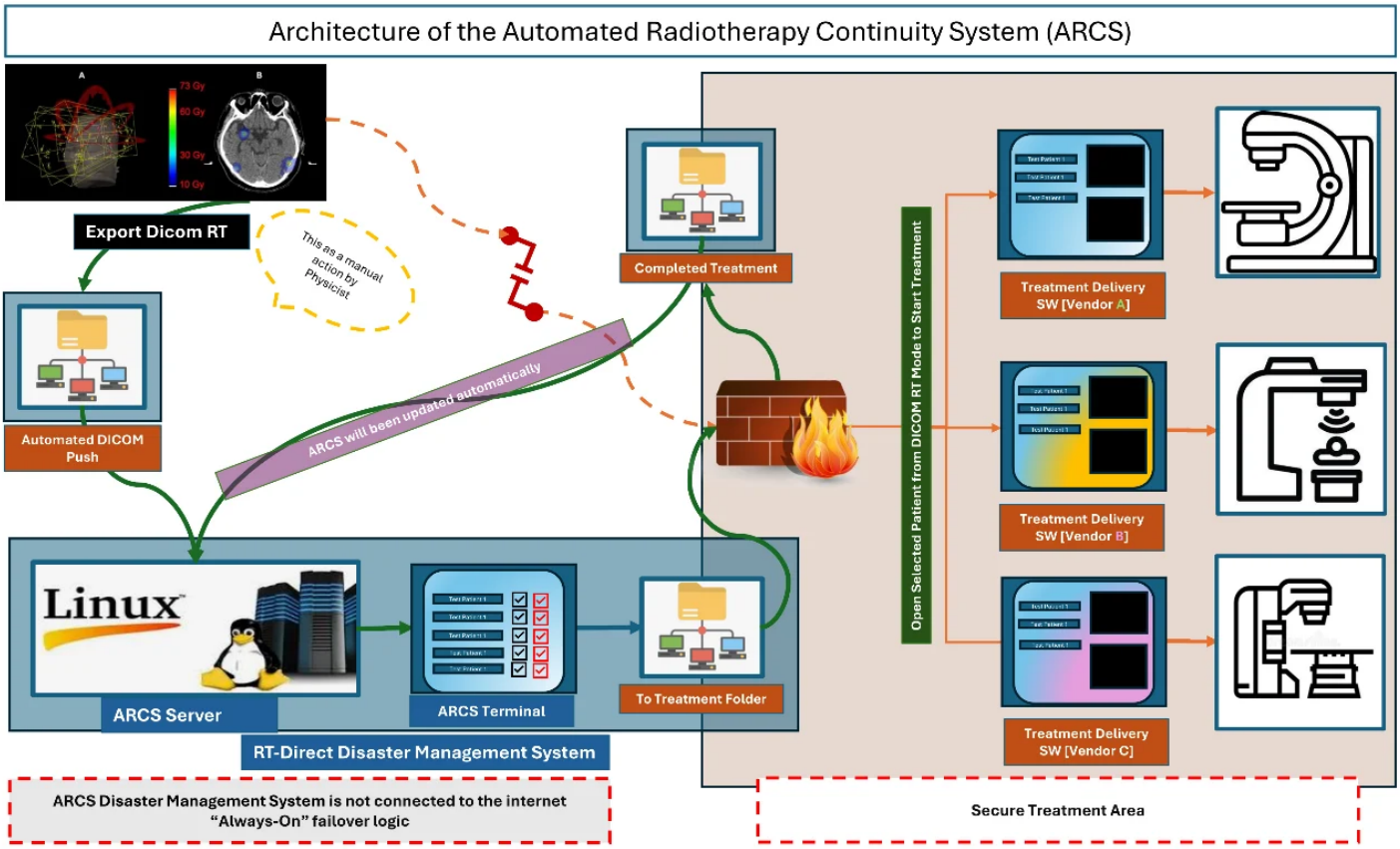
The clinical impact of OIS failure was clearly demonstrated during the 2021 ransomware attack on the Irish Health Service Executive, which disrupted radiotherapy services nationwide and resulted in treatment interruptions for more than 500 patients[3]. Similar risks arise during routine system upgrades or network outages, which may render OIS platforms unavailable for extended periods[4]. International cyber incidents affecting healthcare infrastructure have further highlighted the vulnerability of radiotherapy services to digital system disruption. The 2017 WannaCry ransomware attack impacted multiple hospitals within United Kingdom National Health Service, leading to widespread IT outages that disrupted clinical operations including radiotherapy services. Similar incidents have affected hospitals in Germany, the United States, and Asia, demonstrating that healthcare systems are increasingly targeted by cyber threats[5,6,7]. Because radiotherapy delivery relies on tightly integrated digital workflows, the loss of access to treatment planning and verification systems represents a particularly significant patient safety risk.

Despite growing recognition of these risks, practical and independent solutions to maintain radiotherapy safety during OIS downtime remain limited. Current approaches are often vendor specific or rely heavily on manual intervention[7]. The aim of this study was to design and validate an independent, read-only verification system capable of maintaining safe radiotherapy delivery during both planned and unplanned OIS downtime without modifying clinical data or established treatment workflows. The system described in this study is designed to follow risk-based quality management principles. Such approaches have increasingly been recommended for radiotherapy safety systems. The American Association of Physicists in Medicine Task Group 100 report emphasizes the use of Failure Mode and Effects Analysis (FMEA) to identify and mitigate potential treatment delivery risks in complex radiotherapy workflows. In addition, recent international frameworks addressing radiotherapy cybersecurity resilience highlight the need for independent verification systems capable of maintaining treatment safety during digital system outages[8,9].

# METHODOLOGY

Architecture Design: The Automated Radiotherapy Continuity System (ARCS) was developed as an independent verification platform operating in parallel with the primary OIS. The system is strictly read-only and does not modify treatment plans, dose distributions, structure sets, or delivery parameters under any circumstances. ARCS operates on an isolated server to ensure availability during network failures or cyber incidents affecting the main hospital infrastructure. DICOM-RT objects exported from the TPS are automatically mirrored into ARCS, where they are validated, indexed, and stored for retrieval during downtime events. The overall system architecture and operational states of ARCS are illustrated in Figure 1.

**Figure 1:** Architecture of the Automated Radiotherapy Continuity System (ARCS).



The ARCS architecture is designed to provide a layered verification pipeline that separates data acquisition, validation, and clinical access functions. Incoming DICOM-RT objects are first detected within a monitored export directory and then processed by a validation module responsible for verifying dataset completeness, integrity, and internal consistency. Verified datasets are sequentially indexed and stored within a structured archive, enabling rapid retrieval during downtime events. This architecture allows ARCS to operate independently of the primary OIS while maintaining full compatibility with standard DICOM-RT workflows[9]. To minimize cybersecurity exposure, ARCS operates on a dedicated Linux-based server located within a secured network segment and configured without external internet connectivity. The system interacts with clinical infrastructure only through monitored DICOM export directories and read-only access to treatment delivery log files. This design reduces the risk of system compromise while ensuring that validated treatment data remain available even during major network outages or cybersecurity incidents.

**Risk Analysis:** Risk identification and mitigation were performed using Failure Mode and Effects Analysis (FMEA) in accordance with ISO 14971 principles. Published incident analyses and local downtime simulations were used to identify hazards commonly associated with OIS failure[2,3,8]. Identified hazards included incorrect patient selection, use of outdated or unauthorized treatment plans, incorrect machine assignment, inaccurate fractionation due to missing treatment history, file corruption during manual transfer, and increased human error due to cognitive load. Each failure mode was scored for severity (S), occurrence (O), and detectability (D). The Risk Priority Number (RPN) was calculated as:

$$RPN = S \times O \times D$$

Risk control measures were implemented to reduce occurrence and improve detectability while maintaining clinical severity assumptions. Implementation of the proposed safeguards results in substantial reductions in risk priority numbers (RPNs) across multiple failure modes. Automated verification steps and workflow gating mechanisms reduced the probability of undetected parameter mismatches, thereby significantly lowering the associated risk scores. The identified risks and corresponding mitigation measures are summarized in Table 1:

**Table 1: Failure Mode and Effects Analysis (FMEA) and Residual Risk and residual risk management.**

| Category | Failure Mode | S | O | D | Initial RPN | Control Measure | Residual RPN |
|---|---|---|---|---|---|---|---|
| **Data Integrity** | File corruption during transfer | 8 | 3 | 2 | 48 | SHA 256 verification | 16 |
| **Patient Safety** | Wrong patient treatment | 10 | 2 | 3 | 60 | Dual-identifier check | 20 |
| **Treatment Accuracy** | Incorrect fraction delivery | 10 | 2 | 3 | 60 | Beam-On logging + limits | 30 |
| **System Availability** | ARCS server failure | 8 | 2 | 3 | 48 | High availability + monitoring | 16 |
| **Clinical Governance** | Unapproved plan | 10 | 2 | 2 | 40 | Physics approval gateway | 10 |

Severity scoring was determined according to standard radiotherapy risk-assessment frameworks and reflects the potential clinical impact of treatment parameters mismatches or verification failures. Scores were assigned based on the potential consequences for patient safety and treatment accuracy. Risk mitigation strategies implemented within ARCS focused on introducing independent verification barriers at critical points within the treatment workflow. These safeguards included cryptographic verification of transferred files, automated patient-identifier validation, independent fractionation tracking using treatment delivery logs, and mandatory medical physics approval prior to plan availability during downtime operation. Together, these measures reduce the probability of incorrect treatment delivery while maintaining compatibility with existing clinical workflows.

**Verification Workflow:** During routine operation, the TPS exports DICOM-RT objects to a monitored directory. ARCS automatically detects these exports and verifies file completeness using DICOM Unique Identifiers. File integrity is confirmed using SHA-256 hashing, reducing the risk of data corruption during storage or transfer. All associated DICOM-RT components, including RT Plan, RT Dose, RT Structure Set, and RT Images, are automatically grouped into time-stamped patient folders. Before a plan becomes accessible during downtime mode,

it must be reviewed and approved by a Medical Physicist via a secure web-based interface. Plans remain inaccessible until approval is granted, ensuring clinical governance is maintained during system outages. The verification workflow also includes automated metadata extraction from DICOM objects to validate key treatment parameters, including patient identifiers, treatment machine assignment, beam configuration data, and prescription information. Any discrepancies between expected and detected parameters trigger an automatic validation failure, preventing the affected dataset from becoming available during downtime operation.

In a clinical environment, ARCS is designed to integrate seamlessly with existing radiotherapy workflows without requiring modification to treatment planning or delivery systems. The system operates in parallel with the Oncology Information System using standard DICOM-RT export processes and read-only access to delivery logs. During normal operation, ARCS continuously mirrors and validates treatment data, remaining inactive until downtime conditions occur. Upon OIS failure, ARCS provides immediate access to pre-validated treatment datasets, enabling continuity of care while preserving established clinical safety procedures.

**Patient and Machine Verification:** ARCS continuously verifies patient identifiers, patient names, and linear accelerator assignments using DICOM metadata. Any discrepancy between expected and detected parameters results in automatic blocking of the plan, preventing treatment delivery under unsafe conditions. In addition to DICOM metadata validation, ARCS performs cross-check between treatment planning data and machine delivery logs. These logs contain Beam-ON records that provide an independent record of treatment delivery events. By analyzing the records, ARCS maintains an independent fractionation log that can be used to verify delivered fractions even when the primary Oncology Information System is unavailable.

**Fractionation Control:** An independent fractionation log is maintained using Beam-ON records extracted from delivery logs. Once the prescribed number of fractions has been delivered, further treatment is automatically blocked, preventing over-irradiation and maintaining prescription integrity. Vendor-specific log formats were interpreted using dedicated parsing routines capable of extracting treatment delivery parameters from both Varian and Elekta linear accelerator systems. Although minor formatting differences were observed between vendors, all safety critical parameters required for fractionation verification were successfully extracted and interpreted.

# TESTING AND VALIDATION

Validation testing was conducted on a standalone Linux-based server equipped with 8 GB RAM, a multi-core CPU, and solid-state storage. Only anonymized, publicly available DICOM-RT datasets representative of Varian TrueBeam and Elekta Versa workflows were used. No clinical patient data were processed. All validation was performed using anonymized DICOM-RT datasets, and no live clinical workflows or real-time patient plans were accessed. This methodological decision ensured safe early-phase architecture testing while preserving patient confidentiality and preventing any interaction with ongoing clinical treatments.

The evaluation dataset consisted of 100 treatment plans and was used as a pilot validation cohort to demonstrate technical feasibility and system reliability. This sample size is consistent with early-stage validation studies of safety critical systems, where the objective is to verify deterministic system behavior rather than establish statistical generalization. The inclusion of datasets from multiple vendors (Varian and Elekta) further supports the representativeness of the validation scenario. A total of 100 complete anonymized treatment plans were evaluated. Performance metrics included DICOM-RT mirroring accuracy, metadata extraction time, failover readiness, vendor-specific log parsing reliability, and safety-lock performance. Validation testing also assessed the system's ability to maintain operational continuity during simulated Oncology Information System downtime scenarios. These simulations involved disabling access to the primary OIS while maintaining access to the ARCS validation server, allowing evaluation of system failover behavior and the time required for clinical staff to retrieve validated treatment plans.

# RESULTS

Across all evaluated treatment plans, ARCS achieved a DICOM-RT mirroring accuracy of 99%. Metadata extraction required an average of 20 seconds per patient. Following simulated OIS failure, system failover to downtime mode occurred in under five minutes. Therapists were able to retrieve validated patient plans through the ARCS web interface in under two minutes. Vendor-specific delivery log parsing succeeded in 98% of Varian cases and 94% of Elekta cases. No unsafe irradiation sequences or fractionation errors were observed during testing. Minor inconsistencies observed during vendor-specific log parsing were primarily related to formatting differences in exported log files and did not affect extraction of safety-critical parameters. In all cases where formatting discrepancies occurred, ARCS maintained correct interpretation of Beam-ON events and fractionation counts. A comparison between standard manual downtime procedures and ARCS performance is shown in Table 2.

**Table 2: Comparison Between Manual Downtime Protocol and ARCS.**

| Metric | Manual Downtime Protocol | ARCS |
|---|---|---|
| **Preparation Time** | 15-20 minutes | 30 seconds |
| **Data integrity** | High risk human error | Automated verification |
| **Plan association** | Manual matching required | Automatic UID based matching |
| **Setup documentation** | Difficult to locate during downtime | Instant PDF access |
| **Fractionation safety** | Manual counting | Automated Beam-On completion tracking |
| **Machine matching** | Staff dependent | Automated verification |
| **Overall workflow** | Slow, stressful | Fast and reliable |

ARCS demonstrated robust and consistent interpretation of vendor-specific delivery logs. For Varian machines, parsing succeeded in 98% of cases, with only 2% showing minor format inconsistencies that did not affect safety mechanisms. For Elekta machines, parsing succeeded in 94% of logs, with slightly higher variability due to differences in exported log-file structure. Despite these formatting differences, all essential treatment-verification components were successfully interpreted, and no safety-critical parameters were compromised. The reported performance metrics are presented descriptively to reflect system-level behavior under controlled testing conditions. Because ARCS operates as a deterministic verification system, key performance indicators such as mirroring accuracy, failover time, and safety-lock activation are not subject to stochastic variation in the same manner as clinical outcome studies.

Therefore, descriptive reporting is appropriate for this phase of system validation. Future studies involving larger datasets and clinical deployment will incorporate statistical analysis and variability assessment. For reference, the 95% Wilson score confidence intervals for observed parsing reliability rates are 94.6-100% for Varian log files and 83.5-98.8% for Elekta log files. These figures are provided for transparency and should be interpreted within the context of a pilot validation cohort rather than as population-level estimates.

# Discussion

The ARCS platform addresses a critical vulnerability in modern radiotherapy practice by providing an independent verification layer that remains operational during OIS downtime. By eliminating reliance on manual file transfer and reconstruction, the system reduces cognitive load on staff and minimizes the risk of treatment errors during high-pressure situations[2]. ARCS maintains key safety barriers typically enforced by the Oncology Information System, including patient identity verification, machine-specific plan filtering, independent fractionation tracking, physics approval gating, and DICOM integrity validation. These mechanisms collectively reduce reliance on manual processes while preserving clinical safety during downtime conditions.

These safety mechanisms include:

- Patient identity verification using DICOM patient identifiers and dual-identifier checks
- Machine-specific plan filtering, ensuring therapists only see treatment plans associated with the assigned linear accelerator
- Independent fractionation tracking based on delivery log Beam-ON records
- Automatic prevention of fraction over-delivery once the prescribed number of fractions is reached
- Physics approval gateway requiring medical physics authorization before plans become available during downtime
- File integrity verification using SHA-256 hashing to detect corruption during transfer or storage
- Automatic DICOM UID association ensuring correct linkage between RT Plan, RT Dose, and RT Structure datasets
-

The decision to perform simulation only validation

was deliberate. Because ARCS operates as an independent safety barrier intended for use during OIS downtime, early-stage testing required strict isolation from clinical systems. Simulation with anonymized datasets provided a safe, controlled environment for verifying deterministic behaviors such as identifier matching, DICOM integrity validation, safety lock triggers, and cross vendor log parsing reliability. These behaviors can be robustly evaluated without using live clinical data, in accordance with principles of ISO 14971 and IEC 62304 software development lifecycle. Independent fractionation tracking and mandatory medical physics approval strengthen clinical governance and align with established patient safety principles that emphasize redundancy and independent verification barriers[1]. Unlike vendor-specific backup solutions, ARCS is manufacturer-independent and can be integrated into diverse clinical environments. The increasing frequency of cyber incidents affecting healthcare infrastructure highlights the need for resilient radiotherapy systems capable of maintaining safe operation during digital disruption[5,6,9,10,11,12].

Depending on its clinical use and regulatory jurisdiction, the system could potentially be classified as Software as a Medical Device (SaMD) under regulatory frameworks such as the EU Medical Device Regulation or the U.S. FDA SaMD guidance. The results of this study demonstrate that an independent verification platform can provide meaningful safety benefits without requiring modification of existing clinical treatment workflows. By operating as a read-only verification layer, ARCS avoids potential risks associated with direct modification of clinical treatment data while still enabling rapid access to validated treatment information during system outages[7]. The ARCS architecture also supports scalability in multi-LINAC and multi-site environments. Treatment machine identifiers and institutional metadata extracted from DICOM-RT headers are indexed within the ARCS shadow database and used to dynamically filter treatment plan visibility within ARCS's therapist terminal. This ensures that operators can access only plans associated with their assigned treatment machine, reducing the risk of cross-machine plan selection while allowing multiple treatment units or sites to operate concurrently on the same verification infrastructure. This positions ARCS as a practical and scalable solution for enhancing radiotherapy resilience in modern digital healthcare environments.

## Future Work

A structured clinical implementation pathway is proposed to support safe integration of ARCS into routine radiotherapy practice. Initial deployment would involve controlled pilot implementation within a single institution under medical physics supervision, followed by phased expansion to multi-LINAC environments. Validation during this phase would include parallel operation with the primary Oncology Information System (OIS), allowing comparison of ARCS verification outputs with standard clinical workflows. Subsequent multi-site studies will evaluate system interoperability, workflow integration, and scalability across different institutional settings.

Future work will focus on prospective clinical deployment and evaluation of ARCS in real clinical environments. Multisite validation studies will be required to evaluate scalability, interoperability with diverse treatment planning systems, and integration within larger hospital cybersecurity frameworks.

## Limitations

This study intentionally relied solely on anonymized, publicly available DICOM-RT datasets rather than live clinical data. This approach ensured that all system behaviors including mirror accuracy, metadata verification, fractionation blocking, and failover handling could be validated without interacting with clinical workflows or accessing identifiable patient information. Simulation-based evaluation is appropriate for early-phase safety-critical systems. It enables controlled testing of failure modes that cannot be ethically reproduced in a clinical setting.

## Conclusion

Oncology Information System downtime represents an increasing threat to radiotherapy safety and service continuity. ARCS provides a safe, independent, and read-only verification system that enables continued treatment delivery during both planned and unplanned outages. Validation testing demonstrated high accuracy, rapid failover, and effective prevention of unsafe treatment sequences. The system represents a practical solution for improving resilience and patient safety in modern radiotherapy departments.

**Conflict of Interest:** The authors declare that there is no conflict of interest.

**Funding:** This work received no external funding and was self-funded by the authors.

## References

1. Spezi E, Lewis DG, Smith CW. A DICOM-RT-based toolbox for the evaluation and verification of radiotherapy plans. *Phys Med Biol.* 2002;47(23):4223-32. doi:10.1088/0031-9155/47/23/308.

2. Oliver M, Pearce A, Stillwaugh L, Leszczynski K. The impact of a cyberattack at a radiation oncology department: immediate response and future preparedness. *Adv Radiat Oncol.* 2022;7(5):100896. doi:10.1016/j.adro.2022.100896.

3. Flavin A, O'Neill D, O'Connor M, et al. A national cyberattack affecting radiation therapy: the Irish experience. *Adv Radiat Oncol*. 2022;7:100914. doi:10.1016/j.adro.2022.100914.

4. Vorwerk H, Schmich G, Lishewski P, Adeberg S, Gawish A. Troubleshooting in a digital world-server failure of OIS in radiotherapy from a medical perspective. *Radiation*. 2025;5(2):20. doi:10.3390/radiation5020020.

5. Evans S. Cyberattacks on radiation oncology facilities: protecting your network and patient data. *ASTRO Blog*. 2023 Apr 26. Available from: https://www.astro.org/

6. Keogh RJ, Harvey H, Brady C, Hassett E, Costelloe SJ, O'Sullivan MJ, et al. Dealing with digital paralysis: surviving a cyberattack in a national cancer center. *J Cancer Policy*. 2024;39:100466. doi:10.1016/j.jcpo.2023.100466.

7. 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;21:181-6. doi:10.1002/acm2.12886.

8. Huq MS, Fraass BA, Dunscombe PB, et al. The report of Task Group 100 of the AAPM: application of risk analysis methods to radiation therapy quality management. *Med Phys*. 2016;43(7):4209-62. doi:10.1118/1.4947547.

9. Peters S, O'Donovan A, Bellini M, Caissie A, Coffey M, Dabach A, et al. ESTRO framework for radiation oncology departments to mitigate against cyberattacks. *Radiother Oncol*. 2026;214:111305. doi:10.1016/j.radonc.2025.111305.

10. Yu JB, Dicker AP, Lester-Coll NH, Tsai CJ, Zawalich M. Practical steps to mitigate cybersecurity attacks on radiation oncology practices. *Pract Radiat Oncol*. 2023;13(5):429-33. doi:10.1016/j.prro.2023.05.001.

11. NHS England. Lessons learned from the WannaCry ransomware attack affecting healthcare systems. London: NHS Digital; 2018.

12. International Atomic Energy Agency. Radiation oncology physics: a handbook for teachers and students. Vienna: IAEA; 2005.