radiation

MDPI

Article

Troubleshooting in a Digital World—Server Failure of OIS in Radiotherapy from a Medical Perspective

Hilke Vorwerk [1,2,3,4], Gertrud Schmich [1,2,3,4,5], Philipp Lishewski [1,2,3,4], Sebastian Adeberg [1,2,3,4] and Ahmed Gawish [1,2,3,4,*]

[1] Department of Radiotherapy and Radiation Oncology, Marburg University Hospital, 35043 Marburg, Germany; vorwerk@med.uni-marburg.de (H.V.); gertrud.schmich@uk-gm.de (G.S.); philipp.lishewski@uk-gm.de (P.L.); sebastian.adeberg@uk-gm.de (S.A.)
[2] Department of Radiotherapy and Radiation Oncology, Philipps-University Marburg, 35037 Marburg, Germany
[3] Marburg Ion-Beam Therapy Center (MIT), Department of Radiotherapy and Radiation Oncology, Marburg University Hospital, 35043 Marburg, Germany
[4] University Cancer Center (UCT) Frankfurt–Marburg, 35032 Marburg, Germany
[5] Mildred Scheel Early Career Center, University Frankfurt, 60323 Frankfurt, Germany
* Correspondence: ahmed.gawish@uni-marburg.de

Simple Summary: The increasing reliance on digital systems in radiotherapy has brought significant advancements but also new vulnerabilities. This study addresses the critical issue of server failures in Oncology Information Systems (OISs), which can disrupt patient care and treatment planning. By examining a real-life case of an OIS failure in a radiotherapy department, the authors aim to highlight the challenges posed by these incidents and propose practical solutions for managing them effectively. The research outlines emergency protocols, technical strategies, and clinical workflows to mitigate the impact of such failures and ensure continuity of care. The findings emphasize the importance of preemptive planning, robust data backup systems, and interdepartmental collaboration. This work aims to inspire the development of standardized guidelines that can enhance preparedness and resilience across radiotherapy facilities, ultimately improving patient outcomes and minimizing the risks associated with digital disruptions.

Abstract: The number of server failures, including those in radiotherapy, has dramatically increased over the past 5 years, primarily due to cyberattacks. Despite this trend, many clinics remain unprepared to handle such situations effectively. While it is possible to resolve these issues with thorough preparation and dedicated effort without causing significant interruptions to patient treatments, the process is considerably easier if numerous steps and analyses, both technical and clinical, have already been undertaken. This preemptive work allows for quicker responses and a faster resumption of patient treatments. There are established guidelines on how to prioritize patients and manage total dose in the event of multiple missed treatment sessions. However, many radiotherapy departments in Germany still lack individualized plans for handling software failures. In this article, we describe a failure of the radiotherapy OIS (ARIA by Varian) caused by an interface failure in the Central IT department of the clinic. From this event, we developed a clinical guideline for addressing issues during the outage and identified clinical processes that can be implemented in advance. Our focus was particularly on handling the large volumes of data involved in organizing patient treatments and scheduling. Overall, there needs to be a cultural shift in both the development of technical server infrastructures and the approach to managing OIS failures, as the likelihood of such events increases along with the negative impacts due to increasingly complex treatment plans and software landscapes.

check for updates

Academic Editor: Gabriele Multhoff

Received: 3 September 2024
Revised: 27 April 2025
Accepted: 21 May 2025
Published: 10 June 2025

Citation: 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*, 20. https://doi.org/10.3390/radiation5020020

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Keywords: radiotherapy; cybersecurit; Oncology Information System; digital infrastructure; radiation oncology workflow; emergency planning

1. Introduction

The following article describes a case of an ARIA OIS failure and a derived systematic approach on how to manage a software failure, caused by an OIS independent interface failure in the Central IT department, quickly and efficiently from a clinical perspective.

Total server failure of an Oncology Information System (OIS) in a radiation oncology department such as ARIA OIS or MOSAIQ OIS, although rare in the past, will increasingly occur in clinical routines [1–3]. Historically, total system failures were manageable because radiotherapy treatments often involved simpler, analog techniques. If a software system failed, many aspects of radiotherapy could still be performed manually or with analog methods. For instance, treatment field contours were often realized with mechanical blocks, and primary simulations and manual calculations could temporarily compensate for missing planning capacities. However, with the advent of Intensity-modulated Radiotherapy (IMRT) and other advanced treatment modalities, the dependency on these systems has grown exponentially. Modern radiotherapy treatments cannot be executed without a functional OIS, making any system failure a significant clinical challenge. This challenge extends beyond clinical logistics to impact the increasing use of AI-based tools and radiomics approaches that rely on continuous access to structured digital data. As shown in recent research [4], robust data-handling infrastructures are vital to enable reproducibility and decision support in oncology through AI-driven technologies. Consequently, the challenges posed by software failures today are much more daunting than they were two decades ago. Nevertheless, the clinical emerging issues, especially that care for patients in ongoing treatment and the introduction of new patients to the treatment can be carried out promptly [5], can be approached systematically in the same way.

This article presents a case study of an ARIA OIS failure caused by an interface failure in the Central IT department and the systematic approach developed to manage such failures from a clinical perspective. We outline the steps taken to address the failure, including the immediate response and long-term solutions implemented to prevent future occurrences. The goal is to provide a comprehensive guideline that other radiotherapy departments can adapt to improve their preparedness for similar events. Explanation of Common Technical Abbreviations see Appendix A.

2. Standard Process of the Data Flow

The standard data flow for 3D radiotherapy (RT) plans begins with the generation of CT images (DICOM RT Images) at the CT scanner. These images are typically stored in a virtual buffer, such as a computer folder on a central drive, before being manually, semi-manually, or automatically imported into the treatment planning system (TPS) (Figure 1).

The TPS, which can be integrated with the radiotherapy OIS (e.g., Eclipse TPS integrated with ARIA OIS by Varian), is responsible for generating the target volumes, risk organs, and treatment plans. If external auto-contouring systems are used, they may interface at various stages between the creation of the CT images and the contouring of RT structures by the physician. Regardless of the system, the physician-approved structures ultimately reside in the TPS.

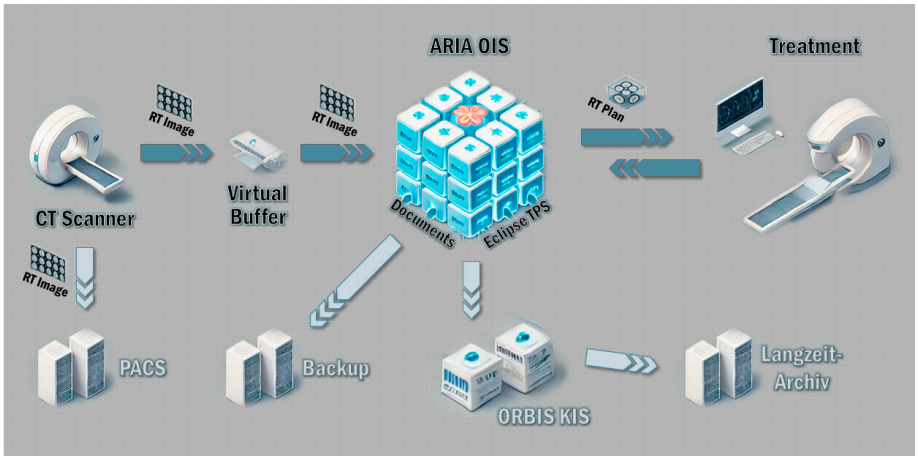


Figure 1. Simplified software map of a radio-oncological department from a medical perspective.

In clinics where the TPS is not integrated with the OIS (e.g., Pinnacle TPS by Philips and MOSAIQ OIS by Elekta), the CT images are imported from the virtual buffer into the TPS. The generated treatment plans are then exported from the TPS and imported into the OIS.

When a patient is to be treated, the OIS communicates with the treatment station, which is the computer at the linear accelerator. Upon selecting the patient at the treatment station, the computer retrieves the treatment data from the OIS and simultaneously locks the patient data in both the TPS and OIS (specifically in the RT treatment data and verification images area) to prevent access by other users. At this point, the treatment station operates independently of the OIS. Direct access to RT data in the OIS is not possible for security reasons. Once the patient completes the treatment, the newly created verification images and the applied dose data are sent back to the OIS, and the lock is lifted.

In addition to RT data, the OIS also contains treatment schedules, appointments, treatment prescriptions, medical documentation, and patient records. If there is an interface to the central Hospital Information System (HIS) (e.g., ORBIS HIS by Dedalus), patient master data and other information such as laboratory values can be directly imported from the HIS into the OIS. Other data are usually entered manually or imported semi-manually from external systems (e.g., digital fax or scanner).

3. Data Storage

Routine backups of the OIS are essential to ensure data integrity and continuity in the event of a system failure. A typical procedure involves automatic daily backups of all data to a backup server. To safeguard against data loss from potential compromises, weekly and monthly updates are also performed and retained for long-term storage. In the event of an OIS failure, the backup server can restore the data to the last backup point, allowing operations to continue with minimal data loss. However, this theoretical scenario is rarely tested in most clinics.

Many clinics now utilize digital long-term archives, where treatment data is stored for up to 30 years. The most commonly used format for long-term storage is PDF/A, which ensures data is stored in a non-editable format resembling printed documents. This format allows for data viewing but not for re-importation into the treatment planning system (TPS) to recalculate previous plans. DICOM format storage, necessary for such recalculations, is generally not supported by long-term archives.

CT images generated during patient planning are not only stored in the virtual buffer but are also archived in a PACS (Picture Archiving and Communication System) for long-term storage. From the PACS, CT images in DICOM format can be retrieved and re-

imported into the TPS for further processing if needed. However, most PACS systems cannot store or process additional DICOM data, such as RT structure and RT dose, which include target volumes and treatment plans. Therefore, long-term archiving of these additional DICOM data outside of the OIS and the backup server remains an unresolved issue in many clinics.

4. Case Report

4.1. Incident Overview

On 18 June 2024, a software error occurred at a university hospital using an ARIA OIS integrated with Eclipse TPS by Varian Medical Systems, running on a Citrix server version. This error initially prevented access to the contoured target volumes of two patients. Although this issue was temporarily resolved by the central IT department of the clinic, a more severe failure emerged on 24 June 2024, rendering the ARIA OIS inoperable and halting all patient treatments.

4.2. Initial Analysis and Response

The first step involved analyzing which components of the OIS had failed and assessing whether any subcomponents were still accessible. The analysis revealed that the failure, originating from the central software error on 18 June 2024, affected all of the Eclipse RT treatment data, medical verification images, and patient documents. Despite some parts of the OIS, such as treatment prescriptions, medical documentation, and schedules, remaining accessible, the decision was made to lock the entire OIS for all users to prevent further errors during the repair process.

4.3. Backup and Restoration Efforts

Upon determining that the original system could not be restored promptly, the team decided to revert to the last available backup from 18 June 2024. However, due to the initial error, regular backups had been suspended, complicating the restoration process. After 48 h, it became evident that restoring the backup would take at least one week. Consequently, the hospital initiated its emergency escalation program, which included prioritizing patients and distributing some to nearby radiotherapy facilities.

4.4. Emergency Measures and Continuity of Care

An in-house emergency solution was established by setting up an OIS on an emergency server, manually entering data for all patients undergoing treatment. Fifteen patients were transferred to nearby clinics to continue their treatments, while the remaining patients were managed using the emergency server. The backup restoration process was completed after 9 days, at which point the backup server was merged with the emergency server, and data from 18 June to 24 June 2024 (229 patients) were manually documented.

4.5. Organizational Challenges and Solutions

One of the significant challenges was maintaining a central point of contact for up-to-date information, as staff members were actively trying to solve problems independently. To address this, a physician and a medical physics expert were designated as central contact points (the organization team) and were present full-time in the central planning room to assist all staff members.

From a medical perspective, creating a prioritization list without access to patient data from the ARIA OIS was challenging. The daily patient treatment list (Germany DIN Report) was digitally stored in the OIS and not directly accessible. However, the approved patient list was stored in the long-term archive in PDF/A format, and this was

used to view the patient list. The diagnoses and planned treatments were accessed from the initial consultation letters, also stored in the long-term archive. The currently applied dose for patients undergoing treatment was retrieved using administrator access, without altering any patient data. This approach mirrors recommendations from other disaster scenarios, such as the Hurricane Maria experience, where proactive documentation and cross-functional coordination were key to maintaining patient care [6].

5. Escalation Levels of an Emergency Plan

An emergency here is defined as an OIS failure with no possibility to perform treatments. When to escalate from one level to the next should be determined by the management team (see below). The management team should meet multiple times a day at fixed times during the entire emergency plan period to determine further procedure.

5.1. Phase 0 Basic Preparation—Analyze Systems, Establish Teams, Test Backups

(Before an emergency occurs; see Figure 2)

(1) Establish a Management Team (see Figure 3)

Form a management team led by the chief physician and lead medical physicist, including representatives from medical, physics, and the outpatient department and radiotherapy technicians (RRT). This team should oversee all emergency planning and execution.

(2) Establish an Organization Team

Designate a central contact point staffed by a specialist physician and a medical physics expert. This team should maintain an up-to-date central Excel list of patients and be available full-time during an emergency.

(3) Establish a Cooperation Team

(4) Pre-arrange agreements with nearby Radiotherapy facilities to continue patient treatments in case of an emergency. Conduct technical tests, such as exporting and importing dummy patient plans, to ensure compatibility (see Table 1).

(5) Discuss Hospital Priority for Server Restoration in an Emergency

Engage in discussions with hospital management and IT to ensure radiotherapy is prioritized appropriately in the hospital-wide emergency plan, just after the laboratory and blood bank.

(6) Analysis of the Software and Server Structure

A basic map of the software and server structure of one's department should be created (analogous to Figure 1). This is particularly relevant for clinics where the TPS is not integrated into the OIS. Based on this, it should be considered which data necessary in an emergency can be retrieved from which software system outside the OIS.

(7) Test the Backup Restoration

Regularly test the backup system to confirm that data can be restored quickly and accurately. Estimate the time required for full restoration.

(8) Test the Possibility to Treat Patients Without OIS Access

Explore alternative methods for continuing patient treatments, such as direct DICOM transfers and paper charting. Develop emergency protocols tailored to the department's software environment.

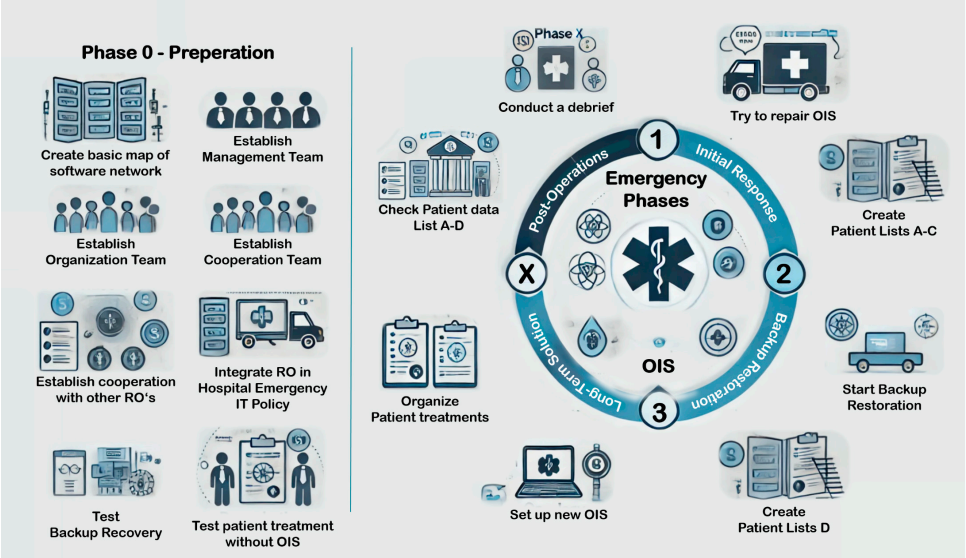


Figure 2. Phases of an emergency program for software failure (for different reasons) from a medical perspective.

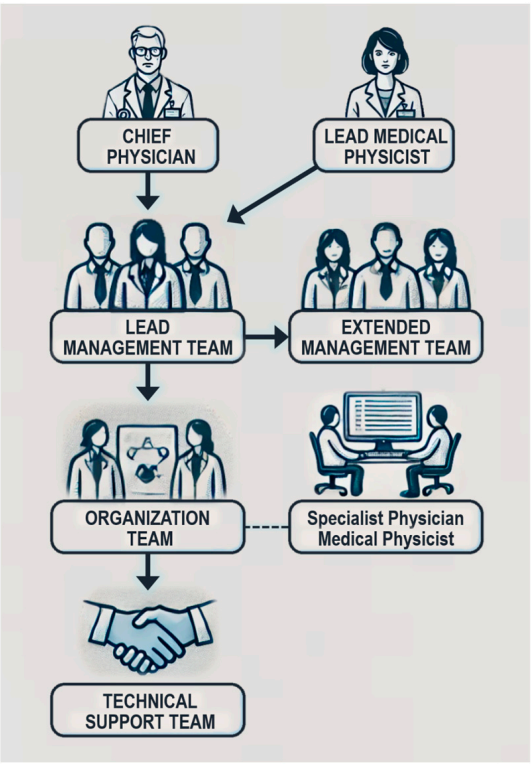


Figure 3. Organization structure during Phase 0 (see Figure 2) from the medical emergency program.

Table 1. Necessary Patient Documents for Continued Treatment in an External Clinic.

Documents	Possible Locations
Short physician's letter requesting patient transfer due to technical defect and inability to complete ongoing treatment in one's clinic	Letter template created in advance outside the OIS
Short certificate with analysis of travel time from the original clinic to the substitute clinic and justification for the insurance	Certificate template created in advance outside the OIS

Table 1. *Cont.*

Documents	Possible Locations
Patient file including diagnosis, disease stage, and course	We recommend storing the patient file at the initial presentation not only in the OIS but, for example, mirroring it to the central HIS system and/or a long-term archive and/or an independent file folder
Original histology	E.g., found in the central HIS system. For external histologies, it is advisable to not only scan them into the OIS but, for example, mirror them to the central HIS system and/or a long-term archive and/or an independent file folder
Chemotherapy prescription and already-applied cycles	We recommend storing the patient file at the initial presentation not only in the OIS but, for example, mirroring it to the central HIS system and/or a long-term archive and/or an independent file folder. Some clinics also use central software systems independent of the OIS and/or HIS
RT treatment prescription with analog signature of a specialist physician	The RT treatment prescriptions embedded in the OIS are usually not exported to other systems. Then, the RT treatment prescription must be manually recreated and approved by a specialist physician for the patient. The total and individual dose of the current treatment plan can be found in the PDF/A format of the treatment plan. Further sequential treatments, e.g., boost treatment, are not found there. It is advisable to integrate the planned dose into the initial consultation letter and then mirror it not only in the OIS but, for example, to the central HIS system and/or a long-term archive and/or an independent file folder. However, the original prescription cannot be retrieved from there
Currently applied dose with analog signature of a specialist physician	E.g., found in the daily list of treated patients (German DIN Report) and should be mirrored to the HIS and/or a long-term archive and/or an independent file folder and/or printed temporarily during the patient RT series. The safest way to document the currently applied dose is still the analog way e.g., as secondary documentation additional to the digital storage.
Copy of informed consent	The informed consent is usually available in analog form or in digital form in a software system independent of the OIS and should be mirrored to the HIS and/or a long-term archive and/or an independent file folder and/or printed temporarily during the patient RT series
Primary positioning documentation	We recommend storing the patient file at the initial presentation not only in the OIS but, for example, mirroring it to the HIS and/or a long-term archive and/or an independent file folder and/or printed temporarily during the patient RT series
Positioning devices, e.g., thermoplastic mask	
Images from the treatment planning CT and diagnostically necessary imaging (e.g., MRI or PET/CT) in DICOM format, e.g., on CD	The CT images are usually stored in the in-house PACS system and can be exported from there in DICOM format
Printout of the treatment plan	It is advisable to create a copy of the treatment plan in PDF/A format, store it in the long-term archive at the time of the plan creation and mirror it to the HIS and/or an independent file folder and/or print it temporarily during the patient RT series. The safest way to document the currently treated RT plan is still the analog way e.g., as secondary documentation additional to the digital storage.

Table 1. *Cont.*

Documents	Possible Locations
Treatment planning including RT dose, RT plan, and RT structure in DICOM format, e.g., on CD	In most clinics, there is no backup of the digital treatment plan in DICOM format either on the backup server or in the PACS system because these can only handle RT images and nothing with RT dose, RT plan, and RT structure. In this case, the printout of the treatment plan must suffice. Some planning systems have the ability to export the treatment planning externally from the OIS in DICOM format with RT dose, RT plan, and RT structure. In these cases, it is advisable to do this as standard.
Patient documents from inpatient stays	The ward documents are usually either in analog form or in a software system independent of the OIS.

5.2. Escalation Level 1 Initial Response—Analyze Failure, Lock OIS, Create Patient Lists

5.2.1. Technical Response

- Involve the department's technical support team and the software manufacturer.
- Assess whether the entire OIS has failed and decide if it should be locked for security reasons.
- Attempt to repair the OIS and verify if backups are compromised.
- Test whether the different backups are involved in failure (e.g., cyberattack on the backup system).

5.2.2. Clinical Response

- Cancel patients in ongoing RT and planned RT for the planned period of escalation level 1.
- If not already done, work through the points from Phase 0.
- Create a patient list (List A) for those undergoing treatment, including necessary details like date of birth, patient ID, diagnosis, etc. This list should be centrally managed by the organization team (see above).
- Create a patient list (List B) for those scheduled to start treatment.
- Assess the feasibility of treatment planning and outpatient work without OIS access, and document these patients (List C).
- Inform cooperation clinics about potential patient transfers and assess their capacity.
- Notify other hospital departments and management that no emergency treatments can be performed.
- Prioritize and reschedule patients from Lists A and B as soon as possible.

5.3. Escalation Level 2 Backup Restoration—Initiate Backup Restore, Prioritize Patients

5.3.1. Technical Response

- Escalate to higher-level technical support.
- Initiate the restoration of the last backup and estimate the time required.

5.3.2. Clinical Response

- Cancel patients in ongoing RT and planned RT for the planned period of escalation level 2.
- Prioritize patients from List A and List B. The prioritization process should be conducted by multiple specialist physicians to ensure fairness and accuracy. A concept for a prioritization list was published by the German radiation protection commission (Strahlenschutzkommission, SSK) [7], which provides detailed guidance on triaging radiotherapy patients during IT system outages.

- Create a sublist of patients from List A for potential treatment at external clinics, considering factors such as travel time, patient mobility, and the need for inpatient treatment.
- Create List D for patients treated between the backup and system failure, documenting all missing information and ensuring data integrity.
- Reschedule and prioritize patients from Lists A and B once the restoration is foreseeable.

5.4. Escalation Level 3 Long-Term Solution—Set up New OIS, Distribute Patients Externally

5.4.1. Technical Response

- Escalate Technical Support to the highest level.
- Explore scenarios with the central IT and OIS manufacturer, including setting up an emergency server.
- If necessary, establish a new OIS with an empty database.

5.4.2. Clinical Response

- Cancel patients in ongoing RT and planned RT for the planned period of escalation level 3.
- Transfer as many patients as possible to external clinics.
- Prioritize and reschedule patients from Lists A and B as soon as possible.

5.5. Phase X Post-Operations—Check Doses, Schedule Patients, Document Failures

Clinical Response

- Review and adjust doses for patients from List A due to the long outage, as necessary [7,8].
- Ensure all patients from Lists A, B, and D have updated treatment appointments.
- Post-document necessary points for patients from List C.
- Document the OIS failure for all patients from Lists A to D.
- Discuss the impact of the software failure with each patient individually.
- Conduct a debrief with the extended management team to analyze shortcomings and implement improvements for future preparedness.

6. Conclusions

The increasing incidence of software failures and cyberattacks on medical software necessitates a proactive and comprehensive approach to emergency preparedness in radiotherapy departments [3,8,9]. The case study of the ARIA OIS failure highlights the critical need for detailed emergency plans that encompass both technical and clinical aspects [10,11]. By developing and regularly testing robust backup systems, establishing clear communication protocols, and fostering cooperation with nearby facilities, radiotherapy departments can minimize the disruption to patient care during software failures. Furthermore, this preparedness lays the groundwork for more advanced clinical workflows, including those involving artificial intelligence, which are particularly sensitive to disruptions in data availability. Recent studies emphasize that medical AI systems—such as those using radiomics to stratify and stage tumors—require stable digital environments to deliver reliable and reproducible results [4]. The failure of such systems could result in delays in personalized treatment planning and staging.

In addition, digital challenges in healthcare extend beyond technical breakdowns. As shown by expert interviews [12], infrastructure deficiencies—such as inconsistent internet access and power interruptions—can exacerbate the effects of software errors. As Joyce et al. highlighted, radiation oncology departments must prepare for complex cybersecurity risks with contingency planning and system hardening [13].

Our case further confirms that digital resilience must include regular process audits, stakeholder cooperation, and system redundancy to prevent chaos during IT outages.

Future efforts should include policy-level strategies to ensure digital healthcare systems are not only innovative but also resilient.

The integration of AI and radiomics into clinical radiotherapy workflows heightens the importance of stable and secure digital systems. As new tools emerge for tumor characterization and treatment optimization, ensuring uninterrupted access to digital data becomes not only a matter of convenience but of clinical efficacy. Future work should address cross-disciplinary standards for digital continuity, including AI model validation under conditions of data disruption, and explore the development of software-agnostic contingency protocols that support intelligent systems in crisis situations.

Radiotherapy departments must prioritize the following steps:

- Routine Testing and Validation: Regularly test backup systems and emergency protocols to ensure rapid and accurate data restoration and continuity of care.
- Centralized Coordination: Designate a central contact point for information dissemination and problem-solving to maintain an organized and effective response during an emergency.
- Cross-functional Collaboration: Engage with IT departments, hospital management, and nearby clinics to ensure radiotherapy is prioritized in hospital-wide emergency plans and that patient transfers can be executed smoothly.
- Proactive Planning: Establish comprehensive guidelines and procedures for handling software failures, including the development of prioritization lists and alternative treatment methods.

By implementing these measures, radiotherapy departments can better prepare for and manage the challenges posed by software failures, ensuring that patient care remains uninterrupted and of high quality. The cultural shift towards greater involvement in software and server infrastructure by clinical staff is essential to adapt to the evolving landscape of medical technology and cybersecurity threats [14,15]. Through diligent preparation and continuous improvement, radiotherapy departments can enhance their resilience against future software disruptions and maintain their commitment to patient safety and treatment efficacy.

Author Contributions: Conceptualization H.V. and A.G.; methodology, H.V.; software, H.V.; validation, P.L. and G.S.; formal analysis, A.G.; investigation, H.V.; resources, A.G.; data curation, H.V.; writing—original draft preparation, H.V.; writing—review and editing, A.G.; visualization, H.V.; supervision, S.A.; project administration, S.A.; funding acquisition, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable. This study did not involve human subjects or identifiable patient data and did not require ethical approval.

Informed Consent Statement: Not applicable. This study did not involve human participants or identifiable patient data.

Data Availability Statement: No new data were created or analyzed in this study.

Acknowledgments: The authors would like to thank the IT department, clinical staff, and management team of the Department of Radiation Oncology at Marburg University Hospital for their support and collaboration during the server failure incident and the development of the emergency protocols described in this manuscript.

Conflicts of Interest: The Authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A

Explanation of Common Technical Abbreviations

HIS (Hospital Information System) [in German KIS = Krankenhaus-Informationssystem]

HIS systems are used for managing, administrating, and documenting electronic patient data. HIS is not a single software but describes all means used for data and information processing within a hospital. An example is ORBIS HIS by Dedalus.

IT (Information System), IMRT (Intensity-modulated Radiotherapy)

OIS (Oncology Information System)

Oncology Information System is software that manages the administrative and clinical aspects of patient data in oncology. It contains the oncology-specific electronic health data of the patient. Many OISs also directly organize and control treatment at the accelerator. Examples are ARIA OIS by Varian Medical Systems and MOSAIQ OIS by Elekta.

OISs generally support the following features:

- Treatment workflow
- Medical prescription for radio-oncological treatment
- Patient register
- Patient documents
- Treatment schedule and appointments
- Financial control
- DICOM RT interoperability
- HL7 interface

TPS (Treatment Planning System)

The TPS is a computer system used to generate an optimal arrangement of treatment fields, energies, field sizes, and escape tendencies for an optimal dose distribution. Examples are Eclipse TPS by Varian and Pinnacle TPS by Philips.

PACS (Picture Archiving and Communication System)

In a digital image management system (PACS), radiological image data are centrally stored and made available for diagnostics within radiology and clinic-wide diagnosis and image distribution.

DICOM (Digital Imaging and Communications in Medicine)

DICOM is a standard format for exchanging data in medicine, e.g., CT, MRI, PET images, and digital X-ray images (RT Image) as well as radiotherapy structures (RT Structure). Besides the image data set, DICOM also contains uniform data fields for patient master data, radiological findings, and examination protocols.

RIS (Radiology Information System)

RISs manage patient master data and patient appointments and are used for entering radiological findings.

References

1. Keogh, R.J.; Harvey, H.; Brady, C.; Hassett, E.; Costelloe, S.J.; O'Sullivan, M.J.; Twomey, M.; O'Leary, M.J.; Cahill, M.R.; O'Riordan, A.; et al. Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center. *J. Cancer Policy* **2024**, *39*, 100466. [CrossRef] [PubMed]
2. Nelson, C.J.; Lester-Coll, N.H.; Li, P.C.; Gagne, H.; Anker, C.J.; Deeley, M.A.; Wallace, H.J. Development of Rapid Response Plan for Radiation Oncology in Response to Cyberattack. *Adv. Radiat. Oncol.* **2020**, *6*, 100613. [CrossRef] [PubMed]
3. 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*, 100896. [CrossRef] [PubMed]
4. Benfante, V.; Salvaggio, G.; Ali, M.; Cutaia, G.; Salvaggio, L.; Salerno, S.; Busè, G.; Tulone, G.; Pavan, N.; Di Raimondo, D.; et al. Grading and Staging of Bladder Tumors Using Radiomics Analysis in Magnetic Resonance Imaging. In *Image Analysis and Processing—ICIAP 2023 Workshops, ICIAP 2023, Udine, Italy, 11–15 September 2023*; Lecture Notes in Computer Science; Foresti, G.L., Fusiello, A., Hancock, E., Eds.; Springer: Cham, Switzerland, 2024; Volume 14366. [CrossRef]

5. Fietkau, R.; Höller, U.; Krause, M.; Petersen, C.; van Kampen, M.; Vordermark, D.; Willner, J. Strukturelle, prozedurale und personelle Voraussetzung für die Erbringung radioonkologischer und strahlentherapeutischer Leistungen 2023 in Deutschland—Ein Positionspapier der Deutschen Gesellschaft für Radioonkologie (DEGRO) [Structural, procedural, and personnel requirements for provision of radiation oncology and radiation therapy services in Germany in 2023-a position paper of the German Society of Radiation Oncologists (DEGRO)]. *Strahlenther. Onkol.* **2023**, *199*, 697–705. [CrossRef] [PubMed]
6. Harrison, A.S.; Sullivan, P.; Kubli, A.; Wilson, K.M.; Taylor, A.; DeGregorio, N.; Riggs, J.; Werner-Wasik, M.; Dicker, A.; Vinogradskiy, Y. 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.* **2022**, *12*, 170–174. [CrossRef] [PubMed]
7. der Strahlenschutzkommission, E. Ausfallkonzepte in der Medizinischen Strahlentherapie. 2018. Ausfallkonzepte. Available online: https://www.aekn.de/fileadmin/inhalte/pdf/Aerztliche_Stelle/strahlentherapie/Ausfallkonzepte_StrlTh_SSK-Empfehlung_2018.pdf (accessed on 25 July 2024).
8. Gay, H.A.; Santiago, R.; Gil, B.; Remedios, C.; Montes, P.J.; López-Araujo, J.; Chévere, C.M.; Imbert, W.S.; White, J.; Arthur, D.W.; 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. *Pract. Radiat. Oncol.* **2019**, *9*, 305–321. [CrossRef] [PubMed]
9. Janssen, S.; El Shafie, R.A.; Grohmann, M.; Knippen, S.; Putora, P.M.; Beck, M.; Baehr, A.; Clemens, P.; Stefanowicz, S.; Rades, D.; et al. Survey in radiation oncology departments in Germany, Austria, and Switzerland: State of digitalization by 2023. *Strahlenther. Onkol.* **2024**, *200*, 497–506. [CrossRef] [PubMed]
10. Flavin, A.; O'Toole, E.; Murphy, L.; Ryan, R.; McClean, B.; Faul, C.; McGibney, C.; Coyne, S.; O'Boyle, G.; Small, C.; et al. A National Cyberattack Affecting Radiation Therapy: The Irish Experience. *Adv. Radiat. Oncol.* **2022**, *7*, 100914. [CrossRef] [PubMed]
11. 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. [CrossRef] [PubMed]
12. Were, M.C. Challenges in digital medicine applications in under-resourced settings. *Nat. Commun.* **2022**, *13*, 3020. [CrossRef]
13. Joyce, C.; Roman, F.L.; Miller, B.; Jeffries, J.; Miller, R.C. Emerging Cybersecurity Threats in Radiation Oncology. *Adv. Radiat. Oncol.* **2021**, *6*, 100796. [CrossRef] [PubMed]
14. U.S. Department of Health and Human Services. Office for Civil Rights. Plan A. . . B. . .Contingency Plan! Available online: https://www.hhs.gov/sites/default/files/march-2018-ocr-cyber-newsletter-contingency-planning.pdf (accessed on 25 July 2024).
15. Yi, B.; Sawant, A.; Chen, S.; Lee, S.W.; Zhang, B. Readiness for Radiation Treatment Continuity: Survey on Contingency Plans Against Cyberattacks. *Adv. Radiat. Oncol.* **2022**, *7*, 100990. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.