2026 JOINT AAPM | COMP MEETING
JULY 19–22 | VANCOUVER, BC

An Implementation of RT Emergency Preparedness System based on a Minimal Disaster Recovery Solution

Lixin Zhan, PhD; Leah Wolfe; Ernest K Osei, PhD
Waterloo Regional Health Network, Kitchener, Ontario

2026 JOINT AAPM | COMP MEETING
JULY 19–22 | VANCOUVER, BC

Introduction

Radiation therapy (RT) program nowadays relies heavily on IT infrastructures. Ransomware keeps being a major threat to health care IT facilities. Other factors, such as natural disasters, technical malfunction, hardware failures etc., can also cause prolonged loss of the whole IT environment. In such a level of IT failure, we lose access to both the oncology information system (OIS) and RT file/image servers. Patient treatment plans will not be accessible and treatments have to be paused for a long time, which could be weeks. CPQR has recently drafted the "Pan-Canadian Radiation Treatment Emergency Preparedness & Cybersecurity Framework" to guide cancer centers in preparing for such extreme situations.

We started our emergency treatment preparation and implemented our solution for our RT program two years ago. Our first implementation was presented in COMP2024. With our system, in a disastrous situation, we are able to continue treatment for patients under treatment or with plans ready for treatment. The initial implementation has the limitation of being only capable of 5 days treatment and works for TrueBeam® 2.7 or lower. With the increased installation of TrueBeam 3.0+ in clinics, the first implementation is not sufficient to provide us ease during disasters any more. Here we present our improved solution which is capable of patient emergency treatment on all kinds of Linacs for ARIA® centric RT program. The similar idea can easily be adapted to RT programs based on other OIS.

Methods and Materials

A brief illustration of our ARIA centric RT+IT infrastructure is shown in Figure 1. In preparing for disaster remediation due to ransomware attacks or other unexpected incidents, we have both the backup and replication (B&R) part for data recovery, and the RT disaster preparedness (RT-DP) part for continuous patient treatment. A reliable B&R solution is critical but it can only maintain data safety. In a wide spread disaster, B&R usually cannot guarantee the recovery of the critical business in a timely manner. RT-DP will be the solution for minimizing negative clinical impact to RT patients.

Linac is capable of treating patients in Queued Mode when OIS is available, or in File Mode without requiring OIS. In a disastrous situation, File Mode is the way to go for treatment. The design of our RT-DP solution was based on File Mode. It contains two modules: the data retrieval module and the treatment module. Both modules are mostly offline and only connect to the network when retrieving or syncing data.

RT-DP data retrieval module automatically updates patient data at a scheduled time. Its working process is illustrated in Figure 2. The treatment module is the solution of seeking for Linac login authentication and RT file access in File Mode when offline. It has two different implementations, v1 and v2. Figure 3 shows v1, our initial implementation, which works for TrueBeam <= 2.7 and other Linacs that don't need domain authentication. When Linac access is not based on live domain authentication and no special file access restriction, v1 can be used. It is easier to set up, maintain and activate.

RT-DP treatment module v2, as illustrated in Figure 4, is our new implementation for Linacs relying on live authentication and has strict file access restrictions, such as TrueBeam 3.0+.

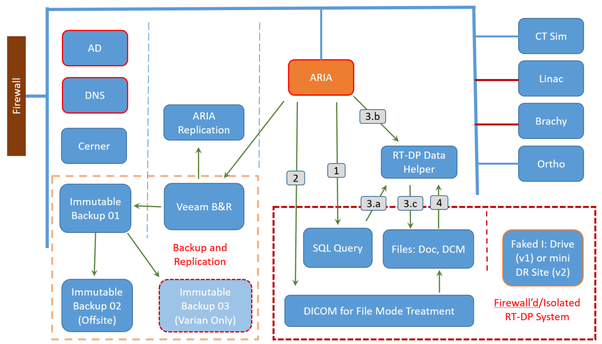

Figure 1. Schematic diagram of RT related IT infrastructure and data safety design from WRHN. Here ARIA stands for all key components for the ARIA system: OIS, Image, DICOM, Platform Service etc.

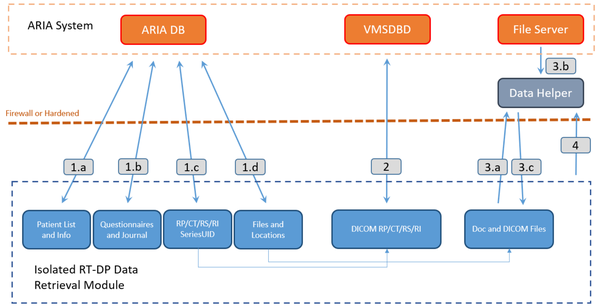

Figure 2. RT-DP data retrieving steps. After NIC is enabled at a scheduled time, 1.a-1.d: SQL queries of Aria DB; 2: DICOM C-MOVE based on SeriesUID queried from step 1.c; 3.a: files copy request based on the result of 1.d; 3.b: file copy from RT file/image server; 3.c: file copy from data helper; 4: send an organized copy of files from all previous steps to data helper. NIC will be disabled after all steps.

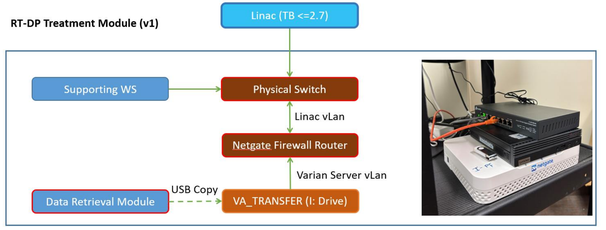

Figure 3. Treatment module v1 connectivity illustration. Only one computer is required to provide VA_TRANSFER share. Authentication relies on cached credentials. This setting works for TrueBeam 2.7 or lower.

Results and Discussion

WRHN has refreshed a few Linacs to TrueBeam 4.1 in the last two years. TB4.1 utilizes live authentication for accessing VA_TRANSFER (I: drive) which is required by File Mode. Cached authentication, as in TB2.7, is not sufficient any more. This asks for the presentation of the Varian Service Platform (VSP), which further relies on the Active Directory (AD) Domain Controller. Hence during emergency treatment, the key servers must exist: VSP, AD, and the VA_TRANSFER share. Our implementation is to set up a minimal disaster recovery (mini-DR) site in a single box virtualization environment (VE).

In this mini-DR site, we virtualize the isolated network to mimic the clinical network, as seen in Figure 5. We also replicate the VSP, VA_TRANSFER, and AD servers to this VE and connect them to the virtual network. This VE server is offline when not in use. Server replica will be refreshed regularly to prevent Trusted Relation Failure. During a disaster, Linac can be connected to the VE box directly so that it can work for File Mode treatment with the most up-to-date treatment files copied from the Data Retrieval module.

Conclusions

We present here our new disaster preparedness solution which is capable of providing emergency treatment for all Linac types with ARIA OIS. This implementation can be easily generalized and adapted to other OIS.

The air-gapped data retrieval module guarantees we have the latest copy of patient data, and the offline treatment module provides a minimal DR solution for treatment continuity during an emergency. Together with departmental emergency policies, it is expected to help minimize unfavorable clinical impacts, even if the whole RT platform is unavailable for a prolonged time.

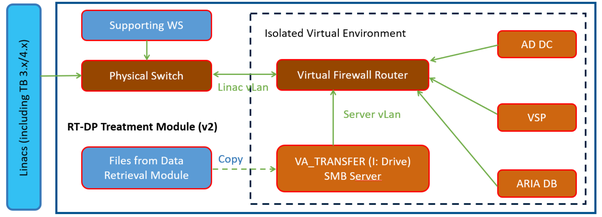

Figure 4. Treatment module v2 connectivity illustration. Servers for Aria DB, VSP, VA_TRANSFER share, together with the domain controller, are replicated into a virtual environment. Also virtualized is a firewall router for VLAN setup and network routing to mimic the clinical network configuration.

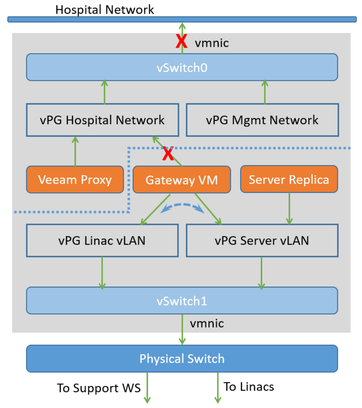

Figure 5. Treatment module v2 network design. Servers are replicated regularly. There should be no network connectivity between vSwitch0 and vSwitch1. Gateway manages the routing between Server vLan and Linac vLan.

Contact

Lixin Zhan
Waterloo Regional Health Network
Email: lixin.zhan@wrhn.ca
Website: https://github.com/lixinzhan
Phone: 519-7494300 x 5428

References

1. CPQR: Pan-Canadian Radiation Treatment Emergency Preparedness & Cybersecurity Framework
2. Varian documents for Aria, Eclipse, TrueBeam, Security and System Preparation
3. VMware vSphere documents for virtualization setup, configuration and maintenance
4. Veeam Backup and Replication infrastructure setup, configuration and maintenance
5. Linux and Windows servers setup, networking, hardening, maintenance, and programming

Further Notes:

- RT-DP is available open source through github: https://github.com/lixinzhan/RT-DP
- **On June 30, 2026, WRHN suffered a hospital-wide failure of domain and network access. RT-DP v1 was successfully applied in clinics and enabled two TrueBeam 2.7 for emergency patient treatment.**