Maryland Experience: Radiation Oncology Contingency Plan against Cyberattacks

Baoshe Zhang, PhD

1

RO Business Continuity Plan

Criteria for a business continuity plan

- Resume radiation therapy within ***24 hours***.
- No any treatment compromise: the same degree of accuracy, the same degree of safety, the same degree of confidence, the same degree of convenience
- Easy to implement
- No extra routine clinical burden
- No worry for data loss
- No need for additional clinical staff training
- A solution for the most disastrous cyberattacks.

2

Infrastructure of Our Solution

Hardware

- A secure data computer (SDC)
- A secondary ROIS computer (SRC)
- SDC and SRC should be a powerful mobile computer, like a gaming laptop

3

Secure Data Computer

- A highly ***customized*** Linux computer.
- ***Bare-bone***: no any unnecessary features and network services and processes and software packages
- Network driver will be ***modularized***
- Auto enable/disable network interface
- ***No remote logon***
- ***Enhanced*** Security Policy

B Zhang etc JACMP(accepted)

4

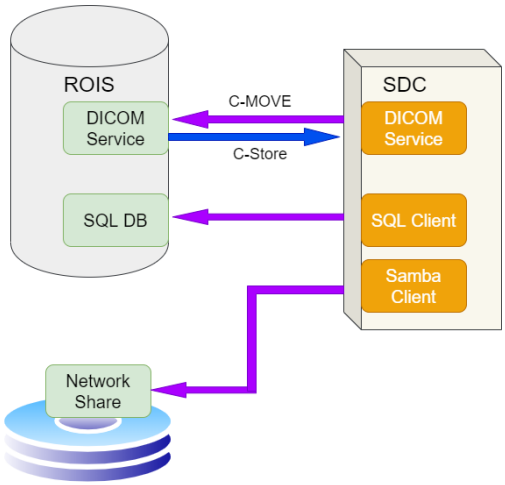
Allowed Network Services/Connection

Incoming network

- DICOM C-Store: to receive DICOM files from ROIS

Outgoing network

- DICOM C-Move: to send out a DICOM request to ROIS
- Windows Network Share
- ROIS SQL DB access
- Email Connection



5

Daily Operation

Major sub-operations

- ❑ *Data Retrieval*
- ❑ *Data Comparison*
- ❑ *Data Verification*
- ❑ *Alerts*

6

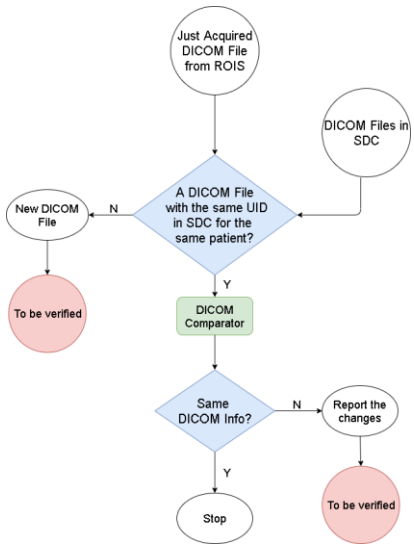
Daily Operation: Data Retrieval

- At 2:00am, turn on the network and its DICOM service.
- DICOM retrieval: SDC initiates a DICOM request to ROIS for DICOM files (Image/Structure/Plan /Dose/ TreatmentRecord) for under-tx patients to the SDC.
- Document retrieval: SDC gets a fresh copy of EMR documents for all the under-tx patients.
- Once SDC gets all the DICOM/EMR files, turn off DICOM service and unload the network driver.

7

Daily Operation: Data Comparison

- Check if DICOM/EMR file is a new one.
- DICOM/EMR file comparison: if the file exists in SDC.
- The SDC will generate a comparison report with detailed changes.
- For any new or changed DICOM/EMR file, SDC will encrypt these files using its own private key.
- Enable the network.
- Email the comparison report to a group of designated recipients and store those encrypted DICOM/EMR files to a network share.
- Disable the network and stay offline

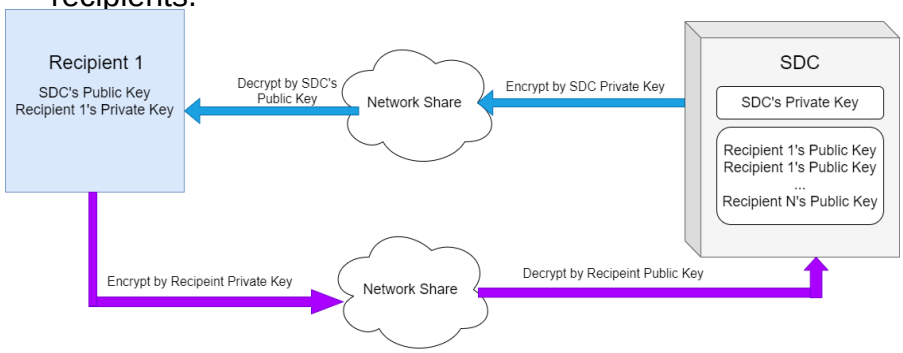


B Zhang etc Phys Med, v69, 28-35(2020)

8

Daily Operation: Data Verification

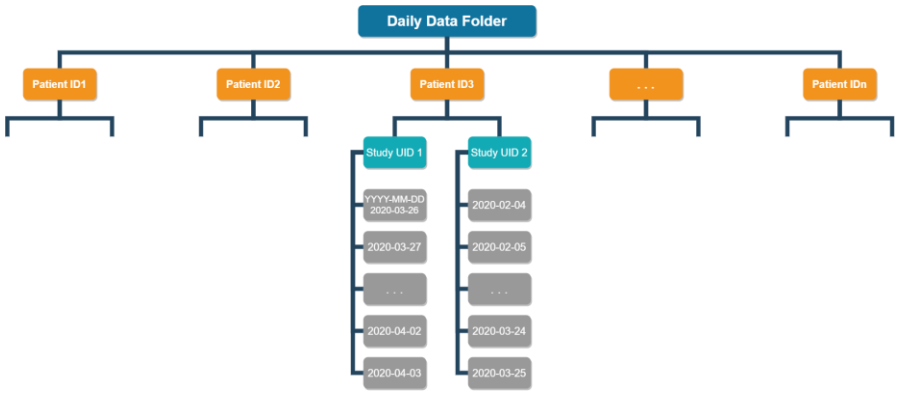
- If there is any change in DICOM/EMR, at least two recipients must verify the change is genuine ***before 10:00am***.
- If none or only one of the recipients verify the changes, the SDC will send out an alert for possible cyberattack ***every 10 minutes*** until the changes are verified by at least two recipients.



9

Daily Operation: Data Storage

Directory Structure



Storage duration

- A patient will be deleted after 30 days since last treatment

10

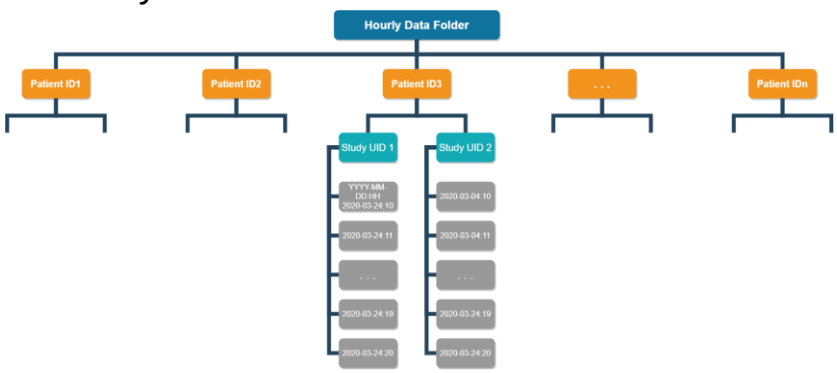
Hourly Operation

- To get ***today's*** treatment history every hour during normal business hours.
- Prevent possible data loss between two consecutive daily operations
- Generation of treatment history PDF report.
- *Tx console computer might keep treatment history for a while.*

11

Hourly Operation: Data Storage

Directory Structure



Storage duration

- These hourly treatment records will only be kept for 48 hrs.
- The PDF treatment record report will only be kept for 48 hrs.

12

Secondary ROIS computer

- Skeleton ROIS Server
  - It has a ROIS SQL DB
  - Machine configurations
  - Beam data/models
  - **No patient-specific data**

- This computer is powered off and secured in a safe place for emergency use

13

SRC upgrade

- SRC needs to be upgraded when
  - *ROIS upgrade*
  - *New machine configuration*
  - *New beam models/beam data*
- This task should be completed by local IT staff

14

Emergency Scenario: launch the SRC

- Once a cyberattack is recognized, the network will be shutdown. The hospital/ department leadership will determine what's next.
- If no other better alternative method will work, this solution will jump in.
- ***ROIS Thick Client*** by the vendor
- ***An isolated network*** by local IT for connection among SRC and ROIS thick client and Tx Control Console
- ***Connection between SRC and Thick Client*** by the vendor

15

Emergency Scenario: launch the SRC

- ***Tx Console Re-Configuration*** by the vendor to use SRC as the ROIS
- ***DICOM/EMR import*** by local physicists/ dosimetrists from the SDC to the SRC
- ***EMR Document Verification and Approval*** by the physicians
- ***Treatment Approval*** by the physicists
- ***Treatment*** by the therapists
- (A couple of weeks) ***Restoring the main ROIS*** from the enterprise backup by local IT and the vendor

16

Emergency Scenario: after the main ROIS is restored

- The cyberattack/virus is disinfected and the main ROIS is rebuilt/verified and contaminated data is removed
- ***DICOM/EMR export*** from the SRC by physicists.
- ***DICOM/EMR import*** to the main ROIS
- ***Removing patient data*** from the SRC.
- Power-off the SRC and secure it for next emergency

17

Results

- All the programs are developed by U. Maryland
- This solution has been implemented for U. Maryland using Varian ARIA.
- With the vendor's assistance, this solution has been tested in our institution successfully.

18

Summary

- A simple business continuity solution and easy to implement
- Safe and robust
- Very cost-effective
- Provide a leeway time for restoring the main ROIS from the enterprise backup system
- No extra clinical burden
- Early detection of virus and ransomware
- If it can be integrated with the enterprise backup system by the ROIS vendor, there will be a ***complete*** business continuity solution for the radiation oncology community

19