Cyberattack fallback scenario for a radiotherapy department

- AZ Klina
- AZ Monica
- AZ Rivierenland
- AZ Voorkempen
- GZA Ziekenhuizen
- UZA
- Vitaz
- ZNA

- **Eric Messens**
- Ali Dabach
- Piet Stevens
- Paul Meijnders
- Koen Snijders
- Dirk Verellen

ISROI-Meeting 2024 – 24 and 25 May 2024 in Freiburg i.Br. Germany

Iridium Netwerk

The Iridium Netwerk is the radiotherapy network of 8 hospitals:
AZ Klina, AZ Monica, AZ Rivierenland, AZ Voorkempen, GZA Ziekenhuizen, UZA , Vitaz en ZNA.

- Radiotherapy Network in Antwerp + Waasland
- 1 main site : GZA Sint-Augustinus (Wilrijk)
- 3 remote sites
  - ZNA Jan-Palfijn (Merksem)
  - VITAZ (Sint-Niklaas)
  - AZ KLINA (Brasschaat)
- Staff:
  - 22 radiation oncologists
  - 21 medical physicists + 2 in training
  - 5 dosimetrists
  - 4 quality managers
  - +60 radiation therapists

Iridium Netwerk

Treatments per year (2023) :
+/- 6500

Linacs :
7 Varian TrueBeam
2 Varian TrueBeam STX

OIS/TPS :
brachytherapy : Aria/Eclipse (Aria is still used for appointment scheduling)
external radiotherapy : RayCare/RayStation since 1/1/2024

Record & Verify :
Varian/Aria

SGRT :
cRAD – Catalyst HD+

Patient QA :
SunCHECK/PerFRACTION (DoseCheck, Fraction 0, Fraction N)

Machine QA :
SunCHECK/SNCMachine

Consequences of a cyberattack

- No access to :
  - HIS/OIS : Patient demographic data : you cannot call a patient to inform him or her that treatments have to be postponed or …
  - OIS/TPS : Patient's treatment data.
  - OIS : List of patients on treatment.
  - OIS : Appointments list.
  - Hospital network and hospital IT infrastructure (pc's, internet, storage, pacs, …)

- Patient's treatments will be interrupted for an undefined time period :
  - A few weeks ?
  - A few months ?
  - Radiobiological effect ? Depends on pathology and patient.
  - Psychological effect for the patient.

Consequences of a cyberattack

- Really bad for the hospital's reputation

- Loss of income for the hospital/department : appr. 10k€ per treatment machine per day

- A lot of stress for all employees, over time,…

- Federal investigation delaying recovery and access to the hospital's IT systems

- …

Working together

Collaboration with BeSTRO :

The BeSTRO is the scientific organisation of radiation oncology in Belgium. Membership is open for radiation oncologists, radiation oncologists in training, radiation physicists, radiobiologists, biomedici, radiation therapists.

Cybersecurity working group

We are working together with the Belgian hospitals to :

- Help each other in setting up a prevention scheme and possible solutions
- Gathering information of existing linacs, treatment accessories, TPS, OIS, …

DPO (data protection officer) working group

- Patient data protection : storing patient data, sharing patient data
- Working on GDPR compliance, Cloud Act,…

ESTRO – ROSQC committee (Radiation Oncology Safety and Quality) :

- Writing panel for cyberattack guidelines (Samuel Peters – Petra Reijnders-Thijssen, …)

Iridium taskgroup for cyberattack prevention

- Paul Meijnders (radiation oncologist)
- Koen Snijders (quality manager)
- Piet Stevens, Ali Dabach, Eric Messens (medical physicists)
- Dirk Verellen (head of medical physicists)
- Anse Boogaerts, Lize Vandersteegen, Peter Berghmans (DPO data protection officers)
- Ivor Dillen, Maarten Maes, Sander Eerdekens, Tom Van Romphey, Ken Bontinck,… (ICT)

Collaborating hospital – AZ Sint Lucas Gent

- Wim Duthoy (radiation oncologist)
- Jan Vandecasteele (medical physicist)

Companies collaborating to find/implement and test solutions

- Siemens - Varian Medical Systems
- RaySearch Laboratories
- Elekta
- MIM Software Inc (GE)
- Dedalus - DobCo

Possible fallback scenarios

Scenario 1 : OIS/TPS completely in the cloud

- ❑ Very expensive
- ❑ To be validated as 100% secure (E2E scenario/tests in case of a cyberattack, disconnected from the hospital network)
- ❑ Out of scope for this presentation

Scenario 2 : Cloud backup combined with collaborating hospitals

- ❑ All treatment data (dicom)
- ❑ Patient demographic data
- ❑ Patient triage list

Scenario 3 : Cloud backup combined with on-premise emergency OIS

- ❑ Test setup is still work in progress
  - ❑ Test setup with Varian
  - ❑ Test setup with RaySearch

- ➢ Scenarios 1&3 depend on the security of the Varian MICAP setup for the linac control system : if compromised ➔ only scenario 2 is possible

Scenario 2

Cloud backup combined with collaborating hospitals

- ❏ Cloud backup solutions :
    - ❏ MIM Pacs + MIM Cloud
        - ❏ In use since +6 months in Iridium

    - ❏ PacsOnWeb

    - ❏ Google Cloud :
        - ❏ DICOM Cloud Healthcare API (REST)

    - ❏ Microsoft :
        - ❏ Azure Health Data Services : Dicom Services

    - ❏ Amazon AWS
        - ❏ Dicom Systems Inc

Scenario 2

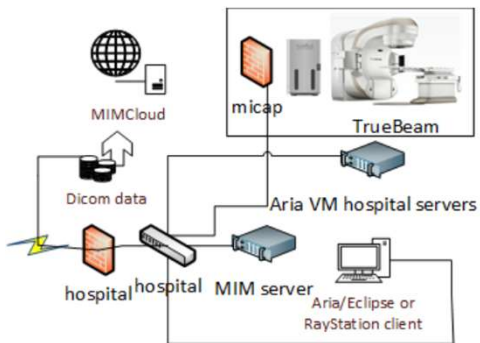**Cloud backup combined with collaborating hospitals**

❑ MIM Pacs + MIM Cloud

    ❑ In use since +6 months in Iridium, automated workflow

    ❑ MIM Cloud costs : 1,128€ per year for up to 500GB of data storage

    ❑ Most important delay in setting up this workflow :

        ❑ MIM Software already had signed a "SUPPLIER AGREEMENT CONCERNING DATA PROTECTION". All are medical software/hardware suppliers have to sign the same agreement.

        ❑ MIM Software had to agree on an addendum to protect the patient data stored in MIMCloud : data storage location in the EU, not US,…

        ❑ This agreement and addenda were validated and approved by our DPO (might be much more difficult for Google Cloud, Azure, AWS solutions)

Scenario 2

Cloud backup combined with collaborating hospitals

- ❑ MIM Software + MIM Cloud

    - ❑ Workflow incorporated in the treatment plan creation workflow

        - ❑ After treatment plan approval the dicom data : RT Dose, RT Plan, RT Struct, CT are send to all dicom destinations : SunCheck, Catalyst, Aria and MIM Pacs from RayStation with a Python script.

        - ❑ The dicom data is send to a separate MIM AE title with a separate patient list/data store combination to isolate the treatment data for our patients in treat and those whose treatment plan is ready.

Scenario 2

Cloud backup combined with collaborating hospitals

- ❑ MIM Software + MIM Cloud

  - ❑ MIM Pacs automatic data mirroring is configured for this MIM cloud patient list so all data is automatically send to MIM Cloud via a secure connection

  - ❑ Every evening a script, started via the task scheduler :
    - ❑ Runs on a virtual server

    - ❑ Scans the OIS database for all active patients

    - ❑ Creates a text file for each patient with his/her demographic data and open/completed treatment fractions with relevant information

    - ❑ Converts these files to pdf

    - ❑ Converts these files to dicom

    - ❑ Sends them to the MIM cloud patient list ➜ mirrored to MIM Cloud.

Scenario 2

Cloud backup combined with collaborating hospitals

- MIM Software + MIM Cloud

    - The same script will also create a triage file :

        - An overview of all patients with the plan name, treatment data and triage code

        - This will be the basis for the patient triage so the radiation oncologist can decide which patients to treat asap and to which collaborating hospital they should be send.

Scenario 2

Cloud backup combined with collaborating hospitals

- ❑ MIM Software + MIM Cloud

  - ❑ Patient data in MIM Patient list and MIM Cloud are removed as soon as the patient's treatment has been completed by sending an HL7 message to MIM Pacs with the patient ID.

Scenario 2

Cloud backup combined with collaborating hospitals

- ❑ RayStation fallback planning has been tested with GZA Varian TrueBeams and Varian TrueBeam of AZ Sint Lucas Gent (Ali Dabach – Piet Stevens – Jan Vandecasteele)
  - ❑ More test with Sun Nuclear ArcCheck have been planned
  - ❑ Replanning takes appr. one hour
    - ❑ RaySearch Labs -> RayStation : Fallback planning (tested)
    - ❑ Varian -> Eclipse : Eclipse Plan Converter (to be tested)
    - ❑ ~~Elekta -> Monaco (no such feature present)~~

- ❑ Assign task group to coordinate workflow after the attack

- ❑ Assign patients to collaborating hospitals using the triage coding

- ❑ Arrange logistics for treatment accessories
  - ❑ Masks
  - ❑ Table accessories
  - ❑ …

Scenario 2

Cloud backup combined with collaborating hospitals

- Triage based on priority level

(Dr. Paul Meijnders)

Priority level	Capacity
1 urgent	10%
2 somewhat urgent	25%
3 standard	50%
4 can wait	80%
5 alternatives available	90%
Brachy Stereotaxy Not indicated above	

- A triage code is entered when the radiation oncologist approves the treatment plan. In Raystation it is possible to edit tags eg. the triage code 1-5. The tags can be defined in the RayStation Clinic settings. They can later be displayed in the patient triage list or via RayIntelligence and used for filtering or used via SQL queries.

Scenario 2

Cloud backup combined with collaborating hospitals

- ❑ Perform E2E test for a test patient in the collaborating hospital with each linac used with different pathologies/treatment types

- ❑ Download patient data from MIM Cloud (MIM Cloud DropBox)

- ❑ Enter patients in OIS of the collaborating hospital

- ❑ Upload treatment data and enter appointments in the OIS

- ❑ Perform patient QA and start treatments

- ❑ Report treatments delivered to affected hospital for updating the patient information systems (HIS, OIS : RT records, plan reports, …)

Scenario 2

Cloud backup combined with collaborating hospitals

- ❑ Limitations :
    - ❑ Number of patients that can continue their treatments is limited
        - ➔ triage
    - ❑ GZA has around +200 patients per day on 9 treatment machines

    - ❑ AZ Sint Lucas Gent
        - ❑ 2 linacs
            - ❑ Varian TrueBeam
            - ❑ Elekta Agility
        - ❑ Will be able to treat 40 of our patients after their normal treatment hours during a limited periode of time (1-2 months ?)

    - ❑ Treatment positioning
        - ❑ SGRT : No cloud storage of treatment positioning data
        - ❑ Different SGRT or positioning systems in the collaborating hospitals
            - ➔ use of more imaging for patient setup
    - ❑ No sharing of patient QA data possible
    - ❑ Different treatment machines, accessories, …

Scenario 3

Cloud backup combined with on premise emergency OIS

- ❑ Cloud backup (eg. MIM Cloud) : using the scenario 2 workflow

- ❑ Installation of an Emergency OIS on a server not connected to the hospital network
  - ❑ Eg. Varian Aria T-Box
  - ❑ Eg. RaySearch RayWorld PVT

- ❑ Separate internet connection

- ❑ Separate network switch/firewall + LTE/4G extender (Fortinet FortiGate + FortiGate extender)

- ❑ Emergency laptops

- ❑ Windows domain controller or setup of local Windows users
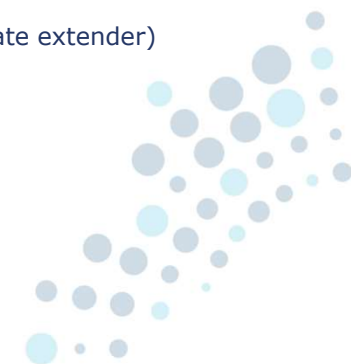
Scenario 3

Cloud backup combined with on-premise emergency OIS

- ❑ Varian : similar to an Aria T-Box
  - ❑ Has agreed to help with this setup and the tests
  - ❑ Has agreed to provide licenses for the test setup
  - ❑ Hardware investment appr. 40k€

- ❑ RaySearch Laboratories : similar to a RayWorld PVT installation
  - ❑ A similar setup has already been tested to perform integration tests with Varian to use RayCare as primary OIS
  - ❑ Reuse hardware for Varian setup

- ❑ Issue to overcome for this setup :
  - ❑ User access to emergency OIS and Varian treatment consoles
    - ❑ Setup of a Windows domain controller and installing/updating active directory users would take 10-20 days which is too much workload for our IT
    - ❑ The use of local users will have to be tested and validated
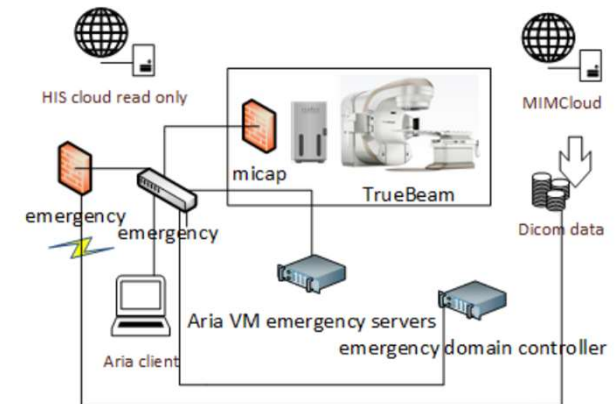
Scenario 2 and 3 combined

Cloud backup combined with on-premise emergency OIS
Cloud backup combined with collaborating hospitals

❑ Treat as many patients as possible with your on-premise emergency OIS

❑ If possible connect your satellite departments via VPN to the emergency OIS and also treat on these linacs

❑ Send the other patients to collaborating hospitals

❑ Efficient triage will be key

Conclusions

❑   A fallback scenario is an achievable goal

❑   RT departments that have scripting support have an advantage by automation
    to speed up the workflow and the treatments

❑   Larger departments will have to rely on more than one collaborating hospital

❑   Collaboration between hospitals is the way to go, sharing tools and experience

❑   Periodical tests of the scenarios is important