# Is your department ready for a cyberattack?

## The first steps for a continuity plan




October, 2026

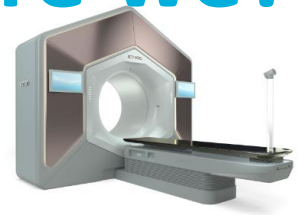
Peter de Graaf
peter.degraaf@radboudumc
+31 6 295 01 932

Radboudumc

# Content

- Who are we?
- Cyber security
  - Introduction
  - Links
  - Reference institute
  - Regulations NIS2
  - Our Business Continuity Plan
  - Implementation

# Who are we?












- Radboudumc in Nijmegen:
  One of the 8 University hospitals in NL
- 2 locations (Radboud + CWZ) both in Nijmegen
- 1 Siemens OpenPro CT
- 2 Elekta linacs
- 3 Varian linacs (Ethos)
- 1 MR-linac
- 1 Flexitron (HDR)
- ≈2500 pt/year
- 5 engineers (self-maintaining)





# In transition ….




2002 first Elekta linac
2012 6th Elekta linac and 7th for research
2020 Elekta Unity MR-linac

2024 change to Ethos (3 linacs) + ARIA / Eclipse

now:
2x Elekta linacs with Aria and VTx interface (TPS Eclipse)
1x Elekta MR-linac with MOSAIQ (TPS Monaco)
3x Ethos

# Cybersecurity

## An increasingly important topic in today's digital world



Een diskette met daarop de eerste ransomware. Uit: Je geld of je gegevens

The first ransomware simply arrived by mail in 1989.

AAMC

Search

Home Resources & Services News Data & Reports Advocacy & Policy

Home / News / The growing threat of ransomware attacks on hospitals

AAMCNEWS

# The growing threat of ransomware attacks on hospitals

Cyberattacks on health care systems have spiked during the pandemic, threatening patient care and private data. Here's how

INNOVATION > CYBERSECURITY

# Attacks On Healthcare Sector Are On The Rise

By David Balaban, Former Contributor. I write about contemporary cybersecurity and online privacy issues.

Published May 30, 2021, 02:11am EDT, Upd

Advances in Radiation Oncology (2022) 7, 100897

ELSEVIER

Radiotherapy and Oncology

Volume 219, June 2026, 111474

Review Article

# Cybersecurity of linear accelerators in radiation oncology beyond ransomwa

Abdulaziz Alhussan [a 1], Mohammad Alhussan [b 1], Nick Chng [c], Frances
Anna Maria Mandalari [b]

HOT ISSUE HOT ISSUE

Clinical Investigation

# Impact of and Response to Cyberattacks in Radiation Oncology

Carl J. Nelson, MD,* Emilie T. Soisson, PhD, Puyao C. Li, MD, Nataniel H. Lester-Coll, MD, Havaleh Gagne, MD, Matthew A. Deeley, PhD, Christopher J. Anker, MD, Lori Ann Roy, MHA, and H. James Wallace, MD

*Division of Radiation Oncology, University of Vermont Larner College of Medicine, Burlington, Vermont*

Received October 19, 2021; accepted December 16, 2021

# Emerging Cybersecurity Threats in Radiation Oncology

Christine Joyce, BS,[a] Faustin Laurentiu Roman, MSc,[b] Brett Miller, MS, MBA,[c] John Jeffries, BS,[d] and Robert C. Miller, MD, MBA, FASTRO[c,*]

[a]University of Tennessee Health Science Center College of M
Auckland, New Zealand; [c]Division of Radiation Oncology, U
Tennessee; [d]Information Security, University of Tennessee M

Received June 28, 2021; revised August 18, 2021; accepted August

**Abstract**

American Hospital Association™

Advancing Health in America

AHA Member Center About Press Center AHA Help

Advocacy Career Resources Data & Insights

# Cybersecurity: Lessons Learned from Ransomware Attack with UVM Health

Contents lists available at ScienceDirect

Radiotherapy and Oncology

journal homepage: www.thegreenjournal.com

ELSEVIER

Original Article

# ESTRO framework for radiation oncology departments to mitigate against cyberattacks

Samuel Peters [a,*], Anita O'Donovan [b], Marcello Bellini [c], Amanda Caissie [d], Mary Coffey [b], Ali Dabach [e], Geoff P. Delaney [f,g,h], Peter E. Fischer [i], Gert Frenken [j], Brian Liszewski [k,l], Philippe Maingon [m], Eric Messens [c], Sophie Perryck [n], Baoshe Zhang [o],
isen [j]

Received: 20 August 2021 | Revised: 20 August 2021

DOI: 10.1002/acm2.13422

EDITORIAL

# Are you ready for a cyberattack?

JOURNAL OF APPLIED CLINICAL MEDICAL PHY

# How 100 hospitals switched to pen and paper to defeat a national cyber-attack

23 June 2026

Joe Tidy

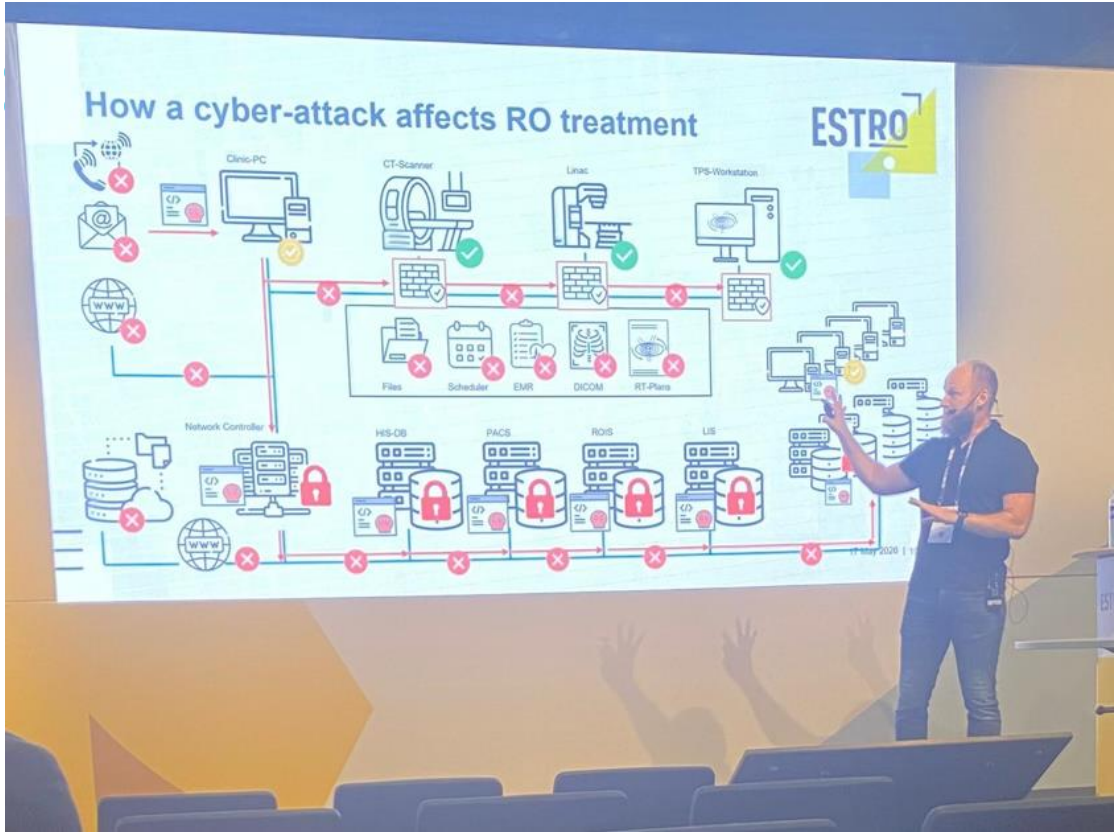
Cyber Correspondent, World Service, Romania

JOURNAL OF APPLIED CLINICAL MEDICAL PHYSICS

MANAGEMENT AND PROFESSION Open Access

# A practical cyberattack contingency plan for radiation oncology

# ESTRO this year



American Hospital Association™
Advancing Health in America

AHA Member Center | About | Press Center | AHA Help Center | Register / Log In | Search AHA...

Advocacy | Career Resources | Data & Insights | Education & Events | News | Individuals & Communities

# Cybersecurity: Lessons Learned from Ransomware Attack with UVM Health

Audio / Podcasts / Advancing Health Podcast

In this special Cybersecurity podcast we have the opportunity to talk to leaders of an AHA member hospital who was a victim of a major ransomware attack in the Fall of 2020. Dr. Stephen Leffler, President and Chief Operating Officer and Dr. Douglas Gentile, Chief Medical Information Officer, join us from the University of Vermont Medical Center in Burlington, Vermont. John previously interviewed them about lessons learned and best practices during the attack which they are willing to share on today's podcast.






https://www.aha.org/advancing-health-podcast/2022-04-06-cybersecurity-lessons-learned-ransomware-attack-uvm-health

# What went down?

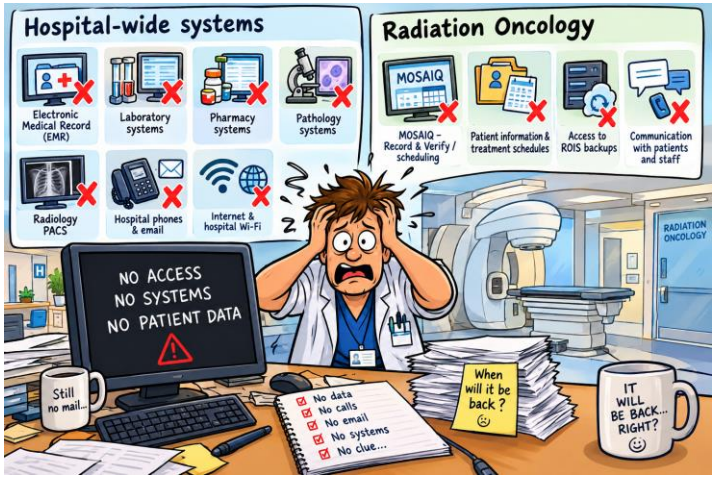



## CYBERATTACK: WHAT WAS NO LONGER AVAILABLE?

**Hospital-wide systems**
- ❌ Electronic Medical Record (EMR)
- ❌ Laboratory systems
- ❌ Pharmacy systems
- ❌ Pathology systems
- ❌ Radiology PACS
- ❌ Hospital phones & email
- ❌ Internet & hospital Wi-Fi

**Radiation Oncology**
- ❌ MOSAIQ – Record & Verify / scheduling
- ❌ Patient information & treatment schedules
- ❌ Access to ROIS backups
- ❌ Communication with patients and staff

**What remained operational**
- ✅ Treatment Planning System (Philips Pinnacle)
- ✅ CT / simulator
- ✅ Linacs
- ✅ DICOM export to local drives




Radiation treatments were cancelled, and patient care was severely disrupted.

# Lessons to be learned

**1. Reconstruct the patient information**

- Paper records and printed schedules
- Patient contact information collected manually
- Treatment history reconstructed

**2. Prioritize patients**

- Patients whose treatment can be postponed
- Patients for whom treatment delay had greater clinical impact

**3. Structured multidisciplinary decision-making**

Clinical IT-specialist / Radiation oncologist / Clinical physicist / (hospital) IT / RTT

The cyberattack was not just an IT problem — it became a patient-care and treatment-continuity problem.

# NIS 2

Network and Information Security 2-guideline



# What is NIS2?

- NIS2 is an EU-wide cybersecurity law designed to raise the level of cybersecurity across Europe.
- It applies to organisations in 18 critical sectors.
- The focus is not only on IT security, but on business continuity and resilience.
- It makes cybersecurity a management responsibility.
- Each EU Member State implements NIS2 through its own national legislation.



# What does NIS2 actually require?

- 1. PREVENT

  Organisations must manage cybersecurity risks.

- 2. DETECT & REPORT

  When a significant cyber incident occurs, organizations must be able to respond quickly.

- 3. TAKE RESPONSIBILITY

  Cybersecurity is no longer something that can simply be delegated to IT.

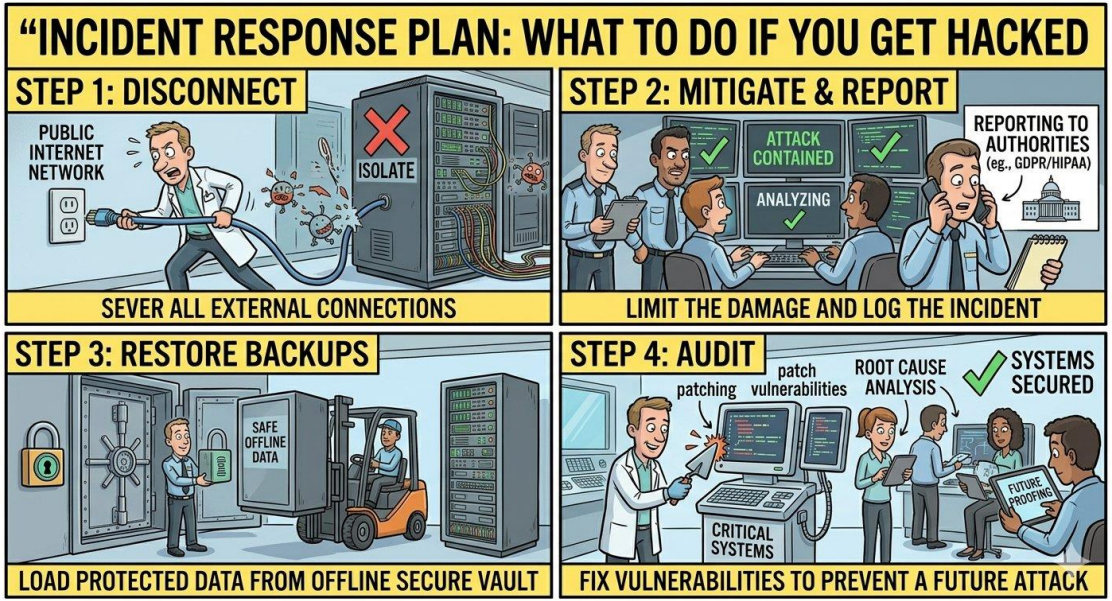
NIS2 changes cybersecurity from “an IT problem” into a business responsibility.

# What does Z-CERT do?

Computer Emergency Response Team




- **Monitors cyber threats** relevant to the healthcare sector
- **Warns healthcare organisations** about emerging threats and vulnerabilities
- **Provides cybersecurity advice and guidance**
- **Supports organisations during cyber incidents**
- **Shares threat intelligence and best practices**
- **Coordinates cooperation between healthcare organisations**
- **Helps improve cybersecurity resilience across the healthcare sector**
- **Provides practical knowledge, tools and training** for healthcare professionals

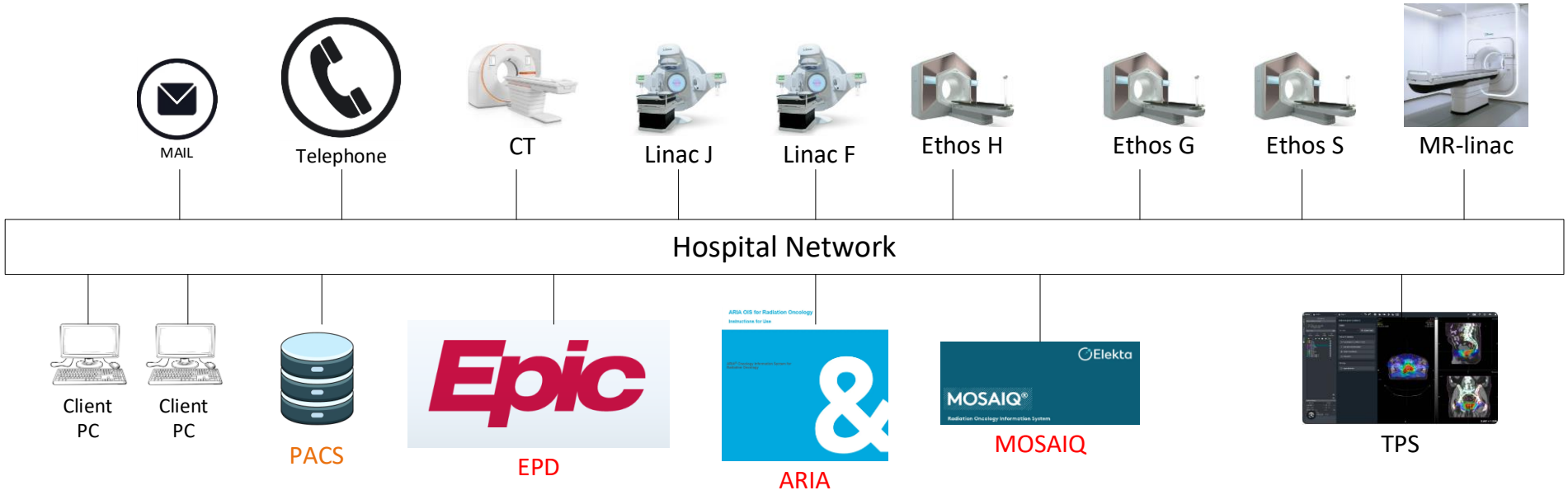



NIS2 →

- PREVENT
- DETECT & REPORT
- TAKE RESPONSIBILITY

# Do Have A Plan!!

# Network at our department




What happens when our data or critical systems are no longer available?

# Radiotherapy Business Continuity Plan

- Ensuring Safe Patient Care During IT Outages
  - Core Principle:

    Patient safety takes precedence over treatment continuity.

    Radiotherapy treatments are only continued when:

    - Reliable patient and treatment data are available
    - Treatment systems are operational
    - Clinical and technical safety can be confirmed
  - Key Principles

    🔒 No treatment without reliable data

    👥 Structured multidisciplinary decision-making

    🔄 Continue treatment where safe, otherwise delay or refer

    📋 Predefined procedures rather than ad hoc decisions

# Scenarios

Scenario 0: < 2 hours → pause and resume
Scenario 1: < 24 hours → adjust daily schedule / 1-day postponement
Scenario 2: 1–7 days → population-wide triage
Scenario 3: > 7 days → structural emergency plan necessary, refer to another institute

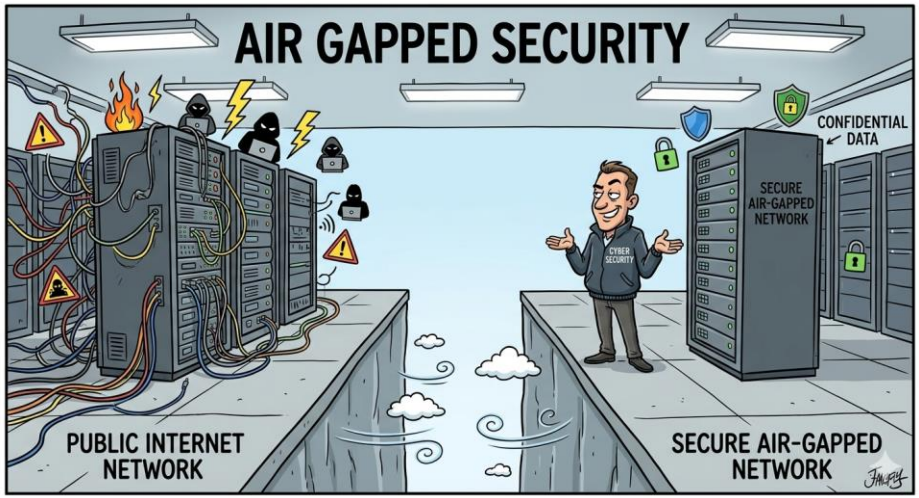
# Patient prioritization

A → non-interruptible
B → interruptible to a limited extent
C → interruptible. Prioritization determined by capacity allocation

# Incident Response Team (IRT)

Clinical IT-specialist → data management & RED-Kit
Radiation oncologist → clinical decision-making
Clinical physicist → physical and technical safety
(hospital) IT → system recovery and technical clearance
RTT → execution

# How to Secure?



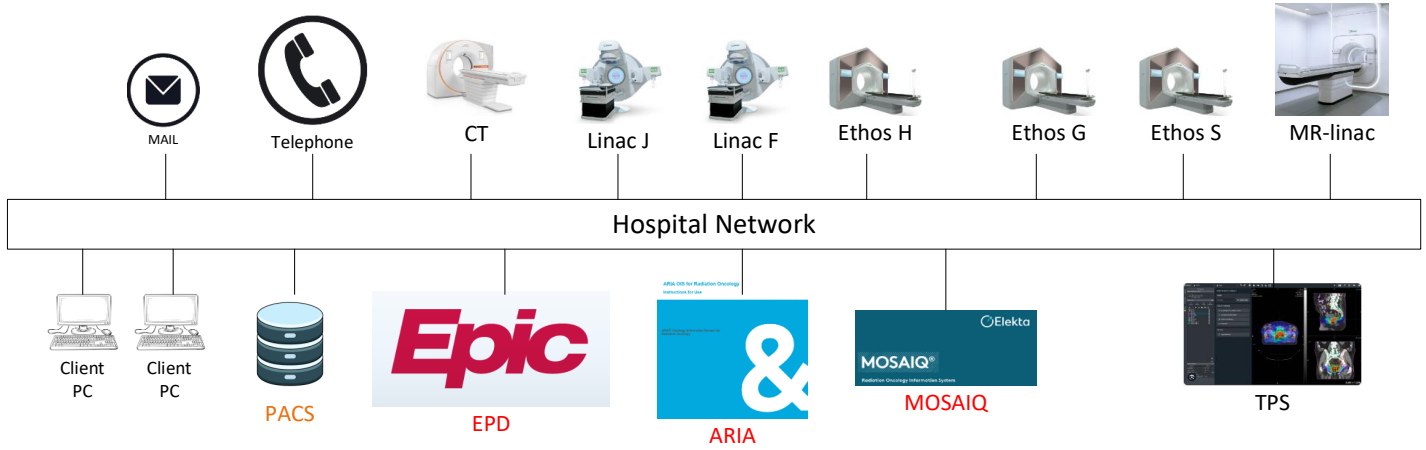

No ‘physical’ connection

Secret - hidding

- e.g. Non-Standard Ports, use port 2222 instead of 22)
- Using a custom encription instead of standard (e.g. AES) encription



# Network at our department




BACKUP

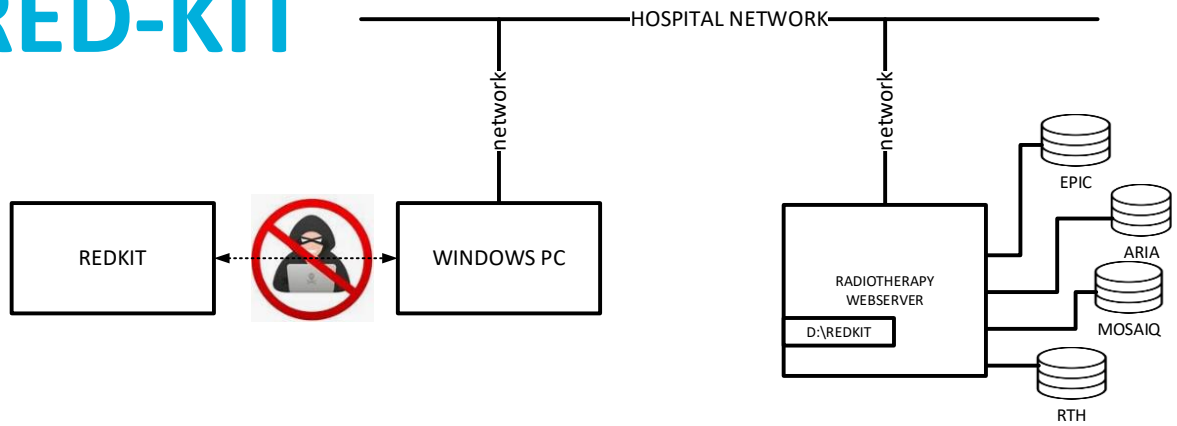
# RED-KIT

- Separate dataset containing essential patient and treatment data
- Immediately available in the event of critical IT system failure
- Supports the Business Continuity Plan
- Enables the secure continuation of treatments of patients
- Enables controlled transfer of patients to another location if necessary



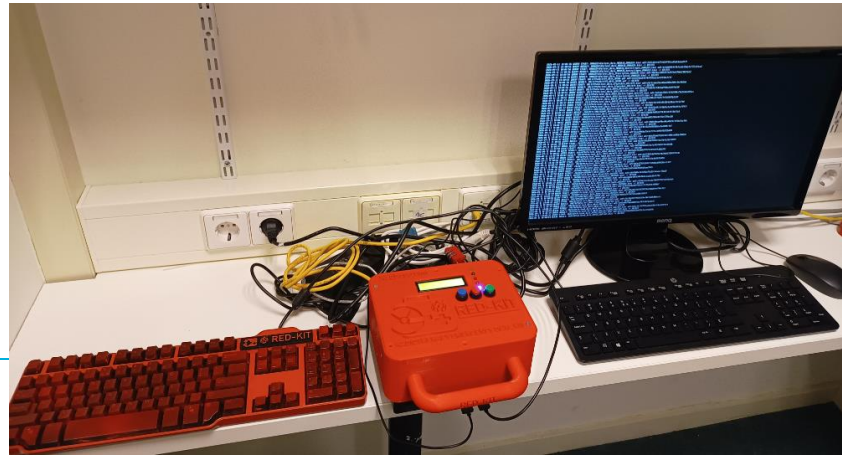

**RED-Kit ensures that critical radiotherapy data remains available when the normal IT infrastructure is unavailable**

# RED-KIT




RECEIVE TRANSMIT COLLECT

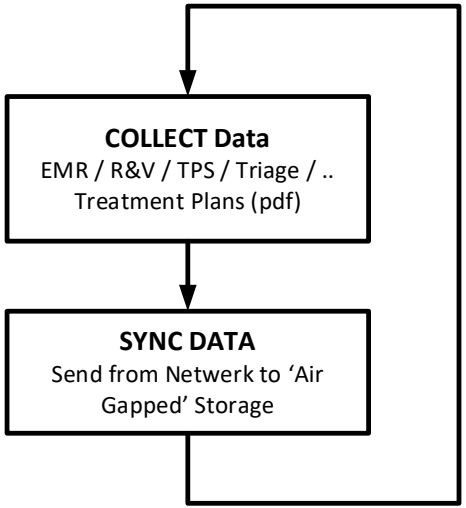


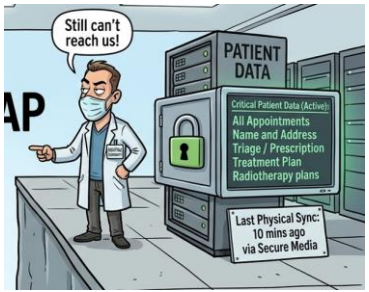



# RED-KIT

- Common Data:
  - All Radiotherapy appointments for the coming 7 days (≈1100 appointments)
  - Info of all patients under treatment at radiotherapy (≈600 pt)

- For each Patient:
  - All patient appointments
  - Name and Address Details and more
  - Triage / Prescription
  - Treatment Plan (only pdf!)
  - Radiation treatments administered
  - Overview, courses, plans, fields…



# Are we Cyber Attack proof?

# (but)We have a plan!







Stay Cyber Safe!
SECURE
CYBER
KNIGHT

# References and links

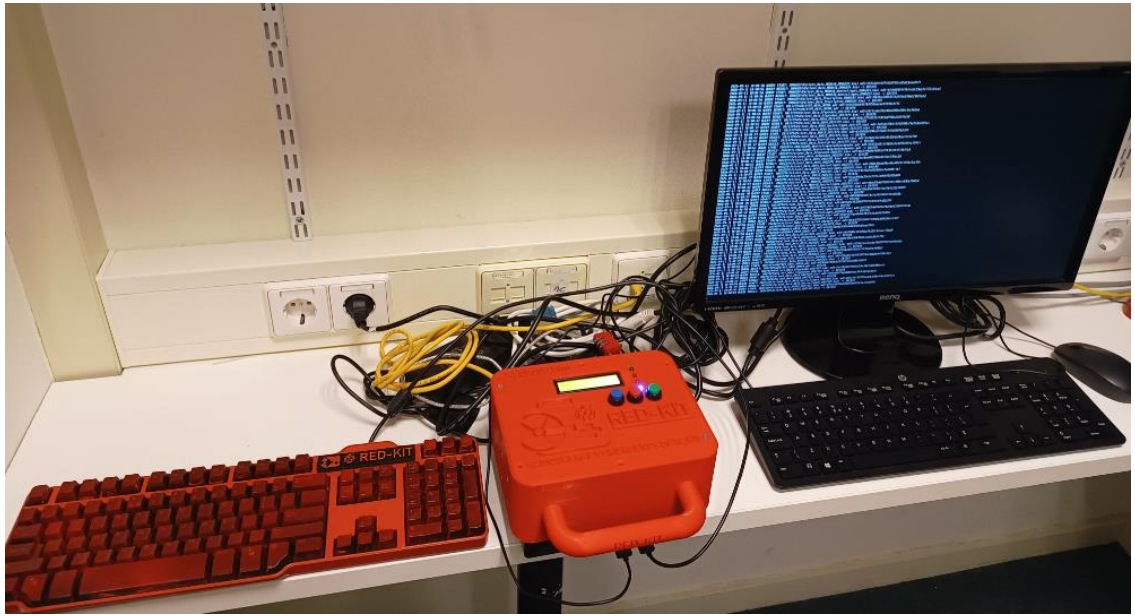

- *ESTRO framework for radiation oncology departments to mitigate against cyberattacks - Radiotherapy and Oncology*
- One Year After a Cyberattack: Lessons Learned and Dosimetric Analysis of Contingency Radiotherapy Plans - International Journal of Radiation Oncology, Biology, Physics
- The growing threat of ransomware attacks on hospitals | AAMC
- Development of Rapid Response Plan for Radiation Oncology in Response to Cyberattack - Advances in Radiation Oncology
- Cybersecurity: Lessons Learned from Ransomware Attack with UVM Health | AHA (podcast)
- Z-CERT publiceert Cybersecuritybeeld: zorg moet rekening houden met langdurige uitval van digitale systemen - Z-CERT
- A practical cyberattack contingency plan for radiation oncology - Zhang - 2020 - Journal of Applied Clinical Medical Physics - Wiley Online Library (Maastro T-Box)
- Are you ready for a cyberattack?
- Attacks On Healthcare Sector Are On The Rise
- Impact of and Response to Cyberattacks in Radiation Oncology
- Emerging Cybersecurity Threats in Radiation Oncology
- Cybersecurity of linear accelerators in radiation oncology beyond ransomware - ScienceDirect

# RED-KIT

- RED-Kit (Radiotherapy Emergency Data Kit)
  - Minimum dataset required for safe continuation of care
    - Clinical information
    - Prescription and treatment status (critical)
    - Technical treatment data
    - Supports local treatment or transfer to another centre

Key Message:
Decisions are driven by data availability, patient priority, and clinical safety, not by operational pressure.

# RED-KIT


RED-KIT


Radboudumc
RED-KIT
RADIOTHERAPY EMERGENCY DATA KIT