

Physical Demonstrator of Medical Imaging Unit: Threat Analysis and Protection Strategies in Cybersecurity

Marina Galiano^{1,2}

¹ CSIRT-CV, Valencia (Spain)

² S2 Grupo (Spain)

Contact email: csirtcv@gva.es

November 2023

- Master's degree in Biomedical engineering by UPV (Valencia, Spain)
- CSIRT-CV, Industrial Cybersecurity (Valencia, Spain)



What is CSIRT-CV?

ICT Security Centre of the Comunitat Valenciana, dependent on Generalitat Valenciana.

CSIRT-CV offers services within the Comunitat Valenciana (Alicante, Castellón and Valencia), with a non-profit public service vocation, so its services are offered free of charge.



Excellence Center of Industrial Cybersecurity

- Industrial Laboratory
 - Honeynet
 - SmartCity
 - Medical Image Unit



Ransomware attack affects 3.3 million patients in California

Giles Bruce - Friday, February 10th, 2023

Report: 'KillNet' targeting hospitals in countries helping Ukraine in war efforts

Naomi Diaz - Thursday, February 2nd, 2023

Healthcare sector should be on the lookout for an aggressive new ransomware tactic

Adam Hawkins, Executive Vice President, Healthcare & Life Sciences, Cydres; Dr. Kall Loper, Vice President, Digital Forensics & Incident Response, Cydres; Shelby Kaba, Director of Special Operations, Cydres - Tuesday, February 14th, 2023

UPDATE: Hackers release more stolen data on dark web from Barcelona's Hospital Clinic

By Chris King - 07 April 2023 - 2:33

Cyberattack disrupts Spanish medicine distribution

📅 MARCH 23, 2023 🧑 DISSENT

MCNA Notifies 8.9M Individuals of Healthcare Data Breach

6 Alabama hospitals affected by CHS third-party breach

Naomi Diaz - Friday, April 7th, 2023

More than 100 dental practices closed for days due to cyber attack

By means of Leon van Poppel
August 5, 2022 2:28 PM - Modified August 5, 2022 2:40 PM

Ransomware scum hit Japanese pharma giant Eisai Group

Some servers encrypted in weekend attack, but product supply not affected

🔴 Julia Kabanus

Fri 9 Jun 2023 - 17:30 UTC

Cerebral Inc. notifying 3,179,835 patients of tracking technologies breach

📅 MARCH 9, 2023 🧑 DISSENT

Feds release new warning concerning KillNet's targeting of hospitals

Noah Schwartz - Thursday, April 6th, 2023

1 million medical records breached in hack of device maker

Noah Schwartz - Tuesday, March 14th, 2023

Alcohol recovery startups Monument and Tempest shared patients' private data with advertisers

📅 APRIL 8, 2023 🧑 DISSENT

New threat group hacked EU healthcare agency and embassies, researchers say

📅 MARCH 15, 2023 🧑 DISSENT

Pennsylvania system: Ransomware gang posted 2,800 patient photos to dark web

Naomi Diaz - Thursday, April 13th, 2023

Phishing incident affects 300,000 individuals at Highmark Health

Giles Bruce - Monday, February 6th, 2023

Cost of data breach in Healthcare



Total cost of a data breach



Figure 1. Measured in USD millions

	2023	2022
1	↑ Healthcare USD 10.93 million	Healthcare USD 10.10 million
2	↓ Financial USD 5.90 million	Financial USD 5.97 million
3	↓ Pharmaceuticals USD 4.82 million	Pharmaceuticals USD 5.01 million
4	↑ Energy USD 4.78 million	Technology USD 4.97 million
5	↑ Industrial USD 4.73 million	Energy USD 4.72 million

Source: IBM. Cost of a Data Breach Report 2023

- Mix of technologies: OT, Medical devices, Medical-grade network and IT

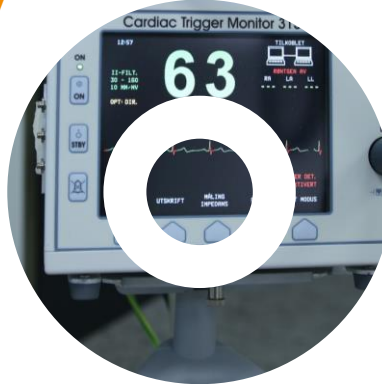


IT, OT, Medical devices and Medical-grade network are nowadays **indivisible**.

Providing **patient safety** is directly related to providing
IT, OT, Medical devices and Medical-grade network **security**.

Main weaknesses in medical devices

- Designed for medical purposes
- No “security by design”
- Unencrypted data
- Hidden functionalities
 - Complex to manage & to set up
 - Default passwords & unknown functionalities
- Bad configurations
- “If it Works, don’t touch it”
- Security by obscurity

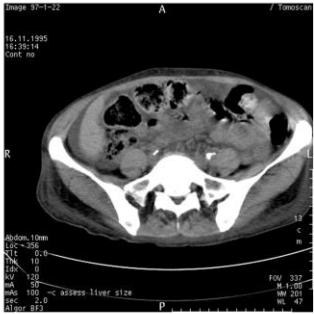


- Expensive devices & long-term life
- Legacy devices
- Outdated OS
- Rented equipment
 - Default passwords
 - Operated remotely
- Trivial passwords
- Mobility inside hospital

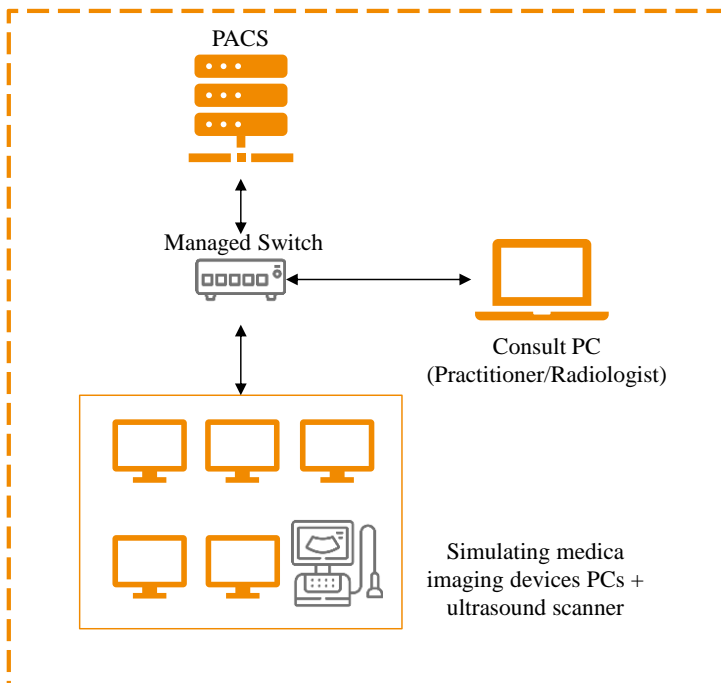
Most disruptive technology in Healthcare



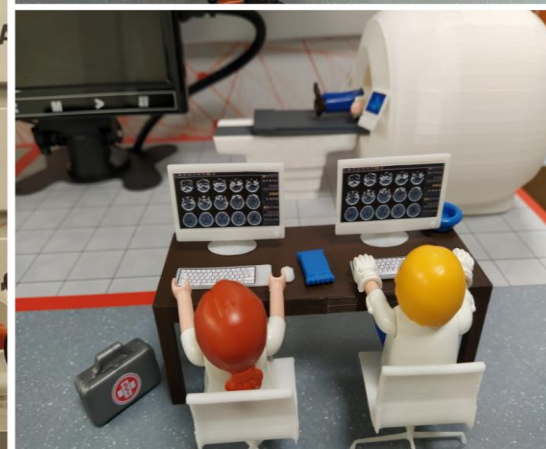



+

Patient		General Equipment	
▶ (0008,1120)	Referenced Patient Sequence	(0009,0070)	Manufacturer
(0010,0010)	Patient's Name	(0009,0080)	Institution Name
(0010,0020)	Patient ID	(0009,0081)	Institution Address
(0010,0021)	Issuer of Patient ID	(0009,1010)	Station Name
(0010,0022)	Type of Patient ID	(0009,1040)	Institutional Department Name
▶ (0010,0024)	Issuer of Patient ID Qualifiers Sequence	▶ (0009,1041)	Institutional Department Type Code Sequence
▶ (0010,0026)	Source Patient Group Identification Sequence	(0019,1090)	Manufacturer's Model Name
▶ (0010,0027)	Group of Patients Identification Sequence	(0019,1099)	Device Serial Number
(0010,0030)	Patient's Birth Date	(0019,1002)	Device UID
(0010,0032)	Patient's Birth Time	(0019,1008)	Gantry ID
(0010,0033)	Patient's Birth Date in Alternative Calendar	▶ (0019,1004)	UDI Sequence
(0010,0034)	Patient's Death Date in Alternative Calendar	(0019,1009)	Manufacturer's Device Class UID
(0010,0035)	Patient's Alternative Calendar	(0019,1020)	Software Versions
(0010,0040)	Patient's Sex	(0019,1050)	Spatial Resolution
(0010,0200)	Quality Control Subject	(0019,1200)	Date of Last Calibration
(0010,0212)	Strain Description	(0019,1201)	Time of Last Calibration
(0010,0213)	Strain Nomenclature	(0019,0120)	Pixel Padding Value
▶ (0010,0216)	Strain Stock Sequence		
(0010,0218)	Strain Additional Information		
▶ (0010,0219)	Strain Code Sequence		
▶ (0010,0221)	Genetic Modifications Sequence		
(0010,1001)	Other Patient Names		
▶ (0010,1002)	Other Patient IDs Sequence		
▶ (0010,1100)	Referenced Patient Photo Sequence		



- Steganography in DICOM
- Modify metadata
- DICOM image modification
- Exfiltration of information
- Export metadata



- Steganography in DICOM
- Modify metadata
- Exfiltration of information
- Export metadata
- DICOM image modification

marina@marina-VirtualBox:/\$ python3 retrieve_patient_data.py

```
# Response Identifier
(0008,0005) CS [ISO_IR 100]
(0008,0052) CS [PATIENT]
(0008,0054) AE [ORTHANC]
(0010,0010) PN [Akamaru]
(0010,0020) LO [A002052]
(0010,0030) DA [19990707]
(0010,0040) CS [M]

# 1 SpecificCharacterSet
# 1 QueryRetrieveLevel
# 1 RetrieveAETitle
# 1 PatientName
# 1 PatientID
# 1 PatientBirthDate
# 1 PatientSex
```

Find SCP Response: 10 - 0xFF00 (Pending)

```
# Response Identifier
(0008,0005) CS [ISO_IR 100]
(0008,0052) CS [PATIENT]
(0008,0054) AE [ORTHANC]
(0010,0010) PN [Armin]
(0010,0020) LO [A000801]
(0010,0030) DA [20131103]
(0010,0040) CS [M]

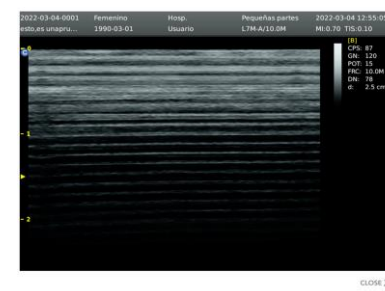
# 1 SpecificCharacterSet
# 1 QueryRetrieveLevel
# 1 RetrieveAETitle
# 1 PatientName
# 1 PatientID
# 1 PatientBirthDate
# 1 PatientSex
```

Find SCP Response: 4 - 0xFF00 (Pending)

```
# Response Identifier
(0008,0005) CS [ISO_IR 100]
(0008,0052) CS [PATIENT]
(0008,0054) AE [ORTHANC]
(0010,0010) PN [Anna]
(0010,0020) LO [AP-6M60]
(0010,0030) DA [20130621]
(0010,0040) CS [F]

# 1 SpecificCharacterSet
# 1 QueryRetrieveLevel
# 1 RetrieveAETitle
# 1 PatientName
# 1 PatientID
# 1 PatientBirthDate
# 1 PatientSex
```

```
0028,0100 (BitsAllocated): 8
0028,0101 (BitsStored): 8
0028,0102 (HighBit): 7
0028,0103 (PixelRepresentation): 0
0028,2110 (LossyImageCompression): 01
0028,2114 (LossyImageCompressionMethod): ISO_10918_1
0041,0010 (PrivateCreator): 54656e676f20707265706172
0041,1001 (Unknown Tag & Data): 61646f20656c206d616c6377617265
7fe0,0010 (PixelData): Null
```



- Use **strong passwords**
- **Encrypt** DICOM **communications**
- Perform **periodic audits** on medical network
- **Monitor** DICOM requests and accesses through web interface
- Network **segmentation**
- Implement **security measures** as firewalls

- Improve cybersecurity **knowledge** of healthcare environments.
- Test in a **real simulated environment**.
- Attack teams can **identify vulnerabilities** and exploit them without risk of causing harm to either facilities or patients.
- Defense teams can **monitor** actions.
- Presentations in conferences, lectures and trainings for cybersecurity **awareness** in healthcare environments.
- **Teach** new professionals how to defend and attack such facilities for ethical purposes.

Thank you!

Questions?



C/ Ramiro de Maeztu N°9 46022 Valencia, España
Teléfono: +34-96-398-5300 Email: csirtcv@gva.es

www.csirtcv.es | csirtcv@gva.es
www.csirtcv.gva.es | www.concientat.gva.es
Facebook.com/csirtcv | X.com/csirtcv

