ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

BIOMEDICAL & CLINICAL ENGINEERING

Healthcare Cybersecurity for Medical equipment

Workshop 06

Dr. Hashem Al-Fadel
January 30, 2024
Cairo, Egypt

Within the 21st International Operations
& Maintenance Conference in the Arab Countries

An Initiative by
OMAINTEC
المجلس العربي للتشغيل والصيانة
Arab Operations & Maintenance Council

Organized by
EXICON.
International Group
مجموعة أكزيكون الدولية

Collaborators
الجمعية العلمية السعودية للهندسة الطبية
Biomed Engineering EGYPT

Agenda

1. Introduction
2. What is health Information security?
3. What is healthcare Cybersecurity ?
4. **The TOP 5 Cybersecurity Threats outlined by HHS**
   (U.S. Department of **H**ealth and **H**uman **S**ervices)

5. Threats to hospitals outlined by ENISA

   (European Union Agency for Cybersecurity)

6. Recommendations, take away message and lessons learned.
7. Reference to Temos standards
8. Questions and answer

Introduction

https://youtu.be/yacOKwzX0ks?si=uw5AkquOP5KvQRQq

Health Information - Definition

According to GDPR (General Data Protection Regulation, European Union, 2018)

The GDPR recognizes **data concerning health** as a special category of data.

Data concerning health means “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”.

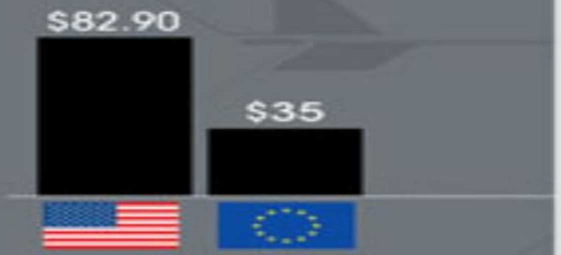
Data protection, more data is sought for sales!

How much is your personal information worth?

http://www.trendmicro.com/ponemon

HEALTH CONDITION

Health condition was much more valuable to U.S. citizens than Europeans, likely due to U.S. healthcare records containing extensive data about individuals, including Social Security numbers.



$59.80

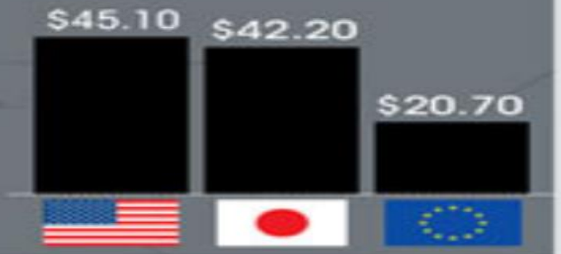
SOCIAL SECURITY NUMBER* *

The Social Security number is unique to the United States (though Japan is soon debuting its own version of this). The Social Security number is a key element in identity theft. But respondents only valued it at $55.70, less than passwords or health condition.

$55.70

PAYMENT DETAILS (credit card)

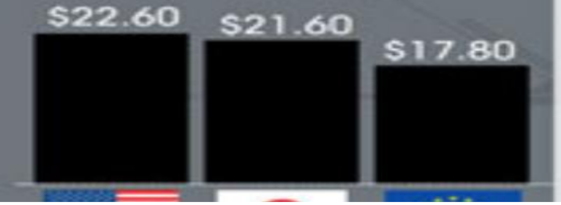
Credit card payment details data was much more valuable to U.S. and Japanese citizens compared to Europeans; this may stem from Europe's long history of using EMV (chip & pin) cards.



$36

PURCHASE HISTORIES

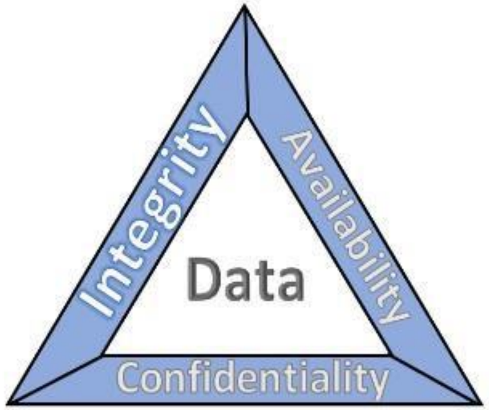
Consumers view purchase history as less valuable than payment details or credit history, but the same can't be said for retailers, who pay handsomely to learn what consumers have purchased (and are



$20.60

Health Information Security - Definition

https://www.nccoe.nist.gov/publication/1800-25/VolA/index.htm

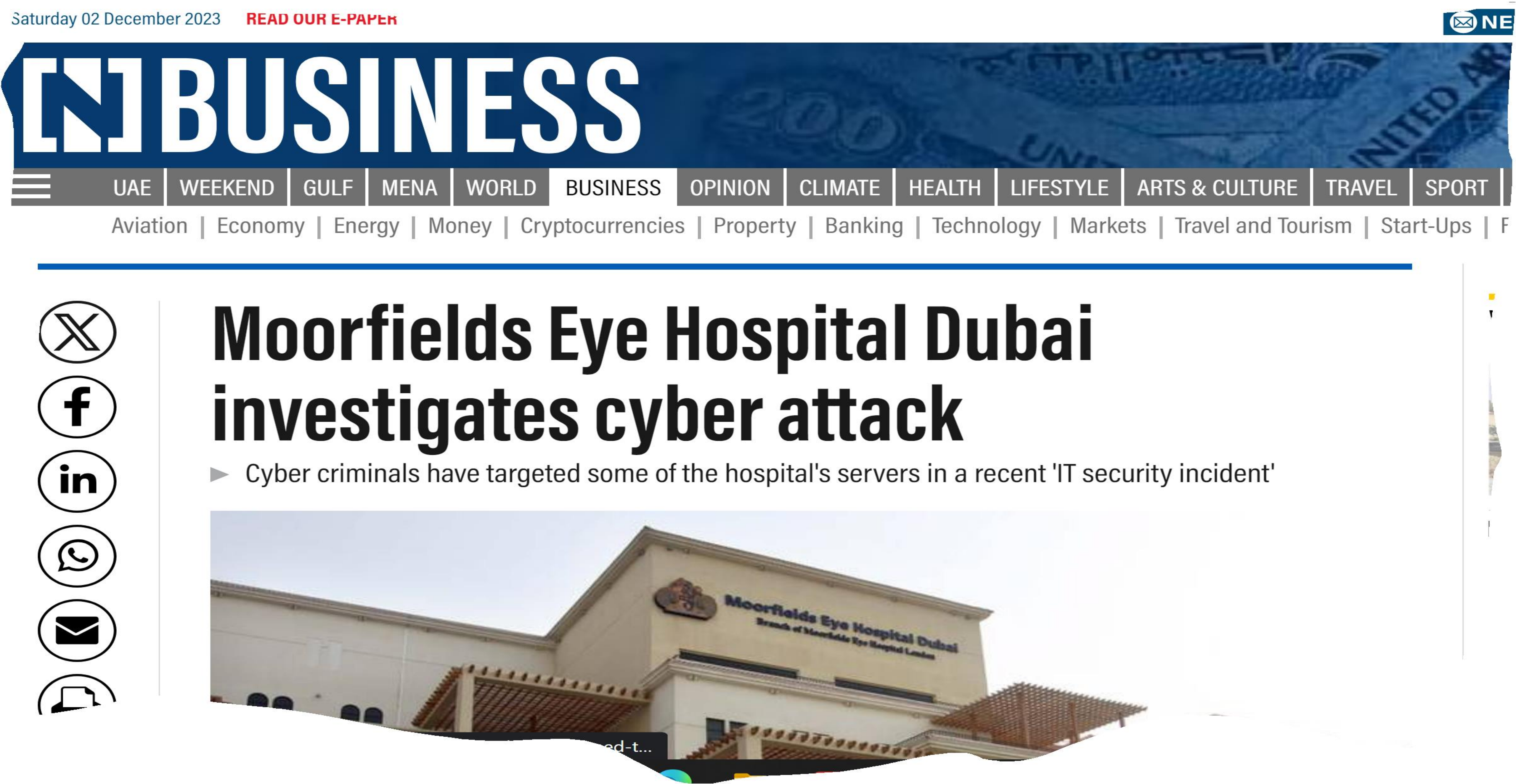


- Confidentiality
  - Personal health data is confidential between patient and physician
  - Goes back to Hypocrites writings.
    - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7132445
  - Privacy and Confidentiality are separate but related, **what is the difference?**
    - https://www.ncbi.nlm.nih.gov/books/NBK236546/
- Integrity
  - All data is protected and whole; nothing is lost, omitted, or damaged.
- Availability
  - Data is available at the time and place of intended use.

News – Headlines

Moorfields Eye Hospital Dubai investigates cyber attack
Cyber criminals have targeted the hospital's servers in a recent 'IT security incident’ taking patient data, it’s under investigation.

Source: N Business



Saturday 02 December 2023 READ OUR E-PAPER

BUSINESS

NE
UAE | WEEKEND | GULF | MENA | WORLD | BUSINESS | OPINION | CLIMATE | HEALTH | LIFESTYLE | ARTS & CULTURE | TRAVEL | SPORT
Aviation | Economy | Energy | Money | Cryptocurrencies | Property | Banking | Technology | Markets | Travel and Tourism | Start-Ups | F
Moorfields Eye Hospital Dubai
Branch of Moorfields Eye Hospital London
ed-t...

Moorfields Eye Hospital Dubai investigates cyber attack

► Cyber criminals have targeted some of the hospital's servers in a recent 'IT security incident'

Introduction – News Headlines

A Major Urban Hospital in ME, Ransomware attack, August, 2023

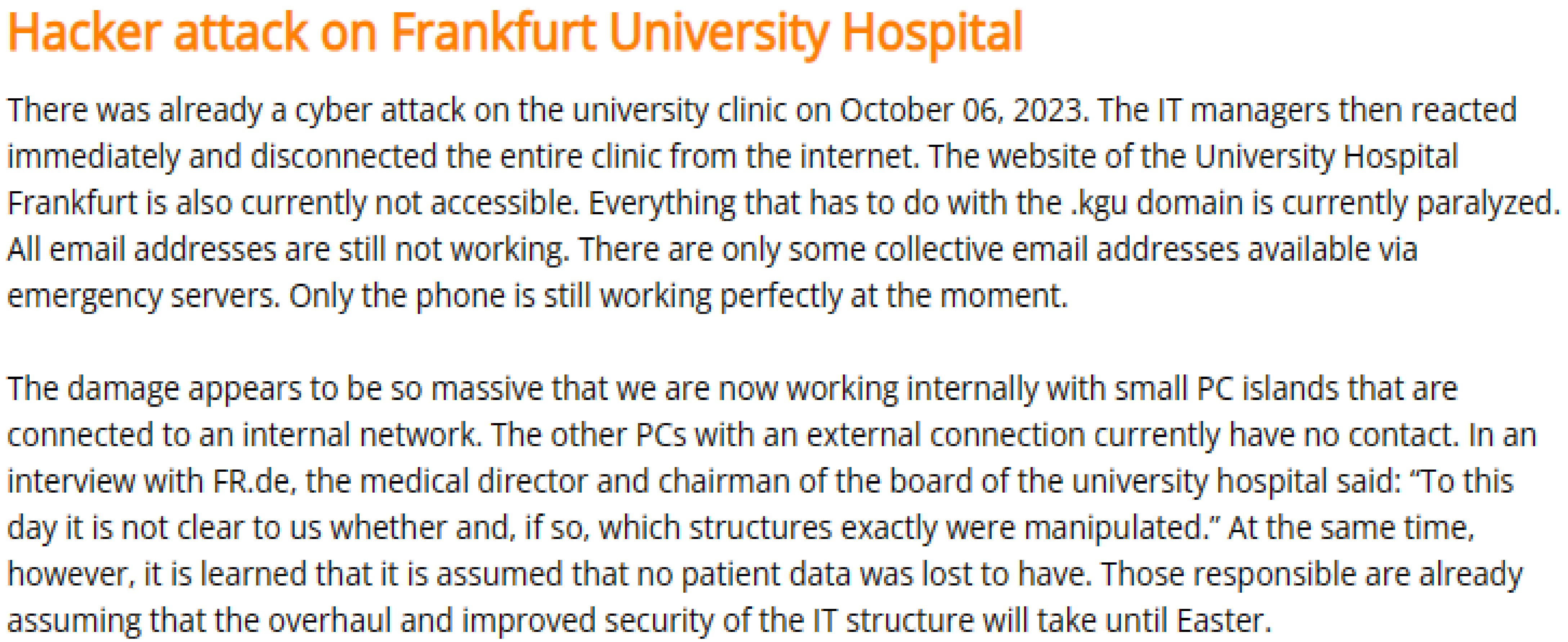
1. Situated in a major urban city in ME
2. Stole 4TB of data includes medical records, personal info, confidential correspondence, financial SQL etc.
3. Suspended patients admission and patients files
4. New patients were directed to nearby facilities
5. Demanded 14 million dollars in exchange for resolving the situation.

Source: CyberGain Dominance, weekly news letter

linkedin.com/pulse/major-urban-hospital-middle-east-faces-ransomware-attack/?trk=article-ssr-frontend-pulse_more-articles_related-c
Search
Home
My Network
Jobs
Messaging
Notifications
Me
For Business
CYBER GAIN
CENTER

Major Urban Hospital in Middle East Faces Ransomware Attack, Highlighting Urgent Need for Cybersecurity Vigilance

Health Information - Definition



Hacker attack on Frankfurt University Hospital

There was already a cyber attack on the university clinic on October 06, 2023. The IT managers then reacted immediately and disconnected the entire clinic from the internet. The website of the University Hospital Frankfurt is also currently not accessible. Everything that has to do with the .kgu domain is currently paralyzed. All email addresses are still not working. There are only some collective email addresses available via emergency servers. Only the phone is still working perfectly at the moment.

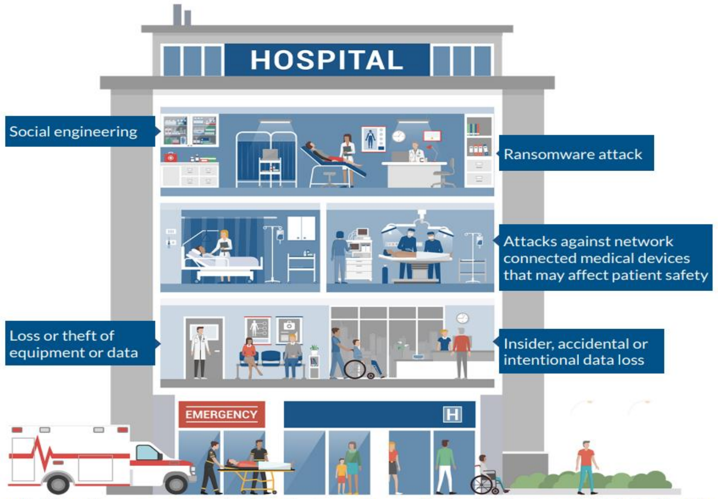
The damage appears to be so massive that we are now working internally with small PC islands that are connected to an internal network. The other PCs with an external connection currently have no contact. In an interview with FR.de, the medical director and chairman of the board of the university hospital said: "To this day it is not clear to us whether and, if so, which structures exactly were manipulated." At the same time, however, it is learned that it is assumed that no patient data was lost to have. Those responsible are already assuming that the overhaul and improved security of the IT structure will take until Easter.

Other Examples: USA

1. VA Cath lab temporarily closure due to Malware infecting computing during interventional cardia procedure
2. Hacking of implantable insulin pump (Radcliff 8/10)
3. Researchers in FDA found Vulnerability identified in PCA3/5 and other infusion pumps (Rios, 5/14-6/15)
4. Medtronic pacemakers recall in the USA
5. **Other examples from your side?**

TOP 5 Cybersecurity Threats

- **Social Engineering**
- **Ransomware**
- **Loss or Theft of Equipment and Data**
- **Insider, Accidental or Intentional Data Loss**
- **Attacks against Network Connected Medical Devices**


HOSPITAL
Social engineering
Ransomware attack
Attacks against network connected medical devices that may affect patient safety
Loss or theft of equipment or data
Insider, accidental or intentional data loss
EMERGENCY
H

The threats portrayed in this graphic are meant to show that these threats can affect organizations in various parts of a hospital and in different healthcare settings. Cyber-attacks can happen anywhere, any time.

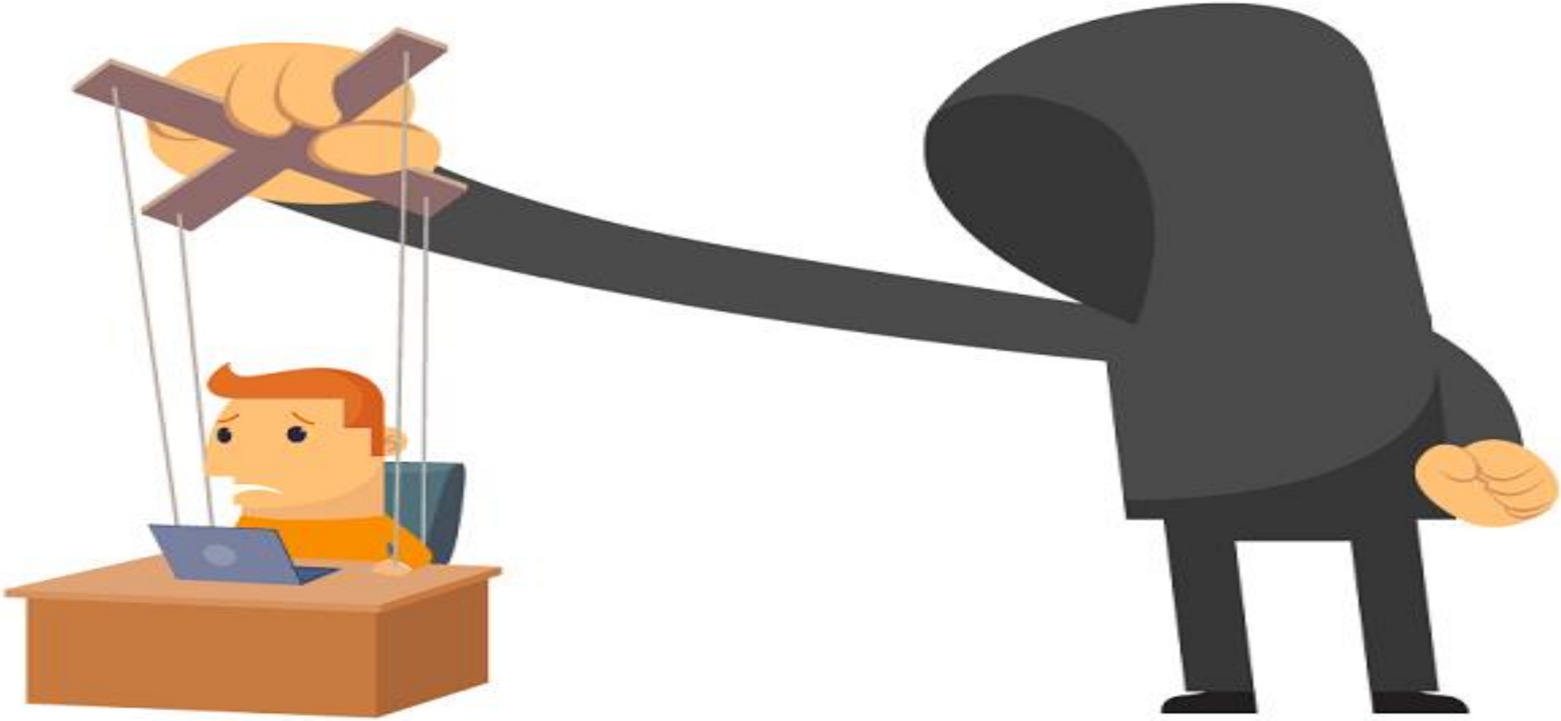
Source:
U.S. Department of Health and
Human Services (HHS) 405(d) Program and Task Group (Inception 2017)
Publication of „Health Industry, Cypersecurity Practises: Managing
Threats and Protecting Patients“ (HICP)

TOP 5 Cybersecurity Threats

- **Social Engineering**
- Ransomware
- Loss or Theft of Equipment and Data
- Insider, Accidental or Intentional Data Loss
- Attacks against Network Connected Medical Devices

What is Social Engineering?

The art of manipulating people so that they give up confidential information or break standard security practices.

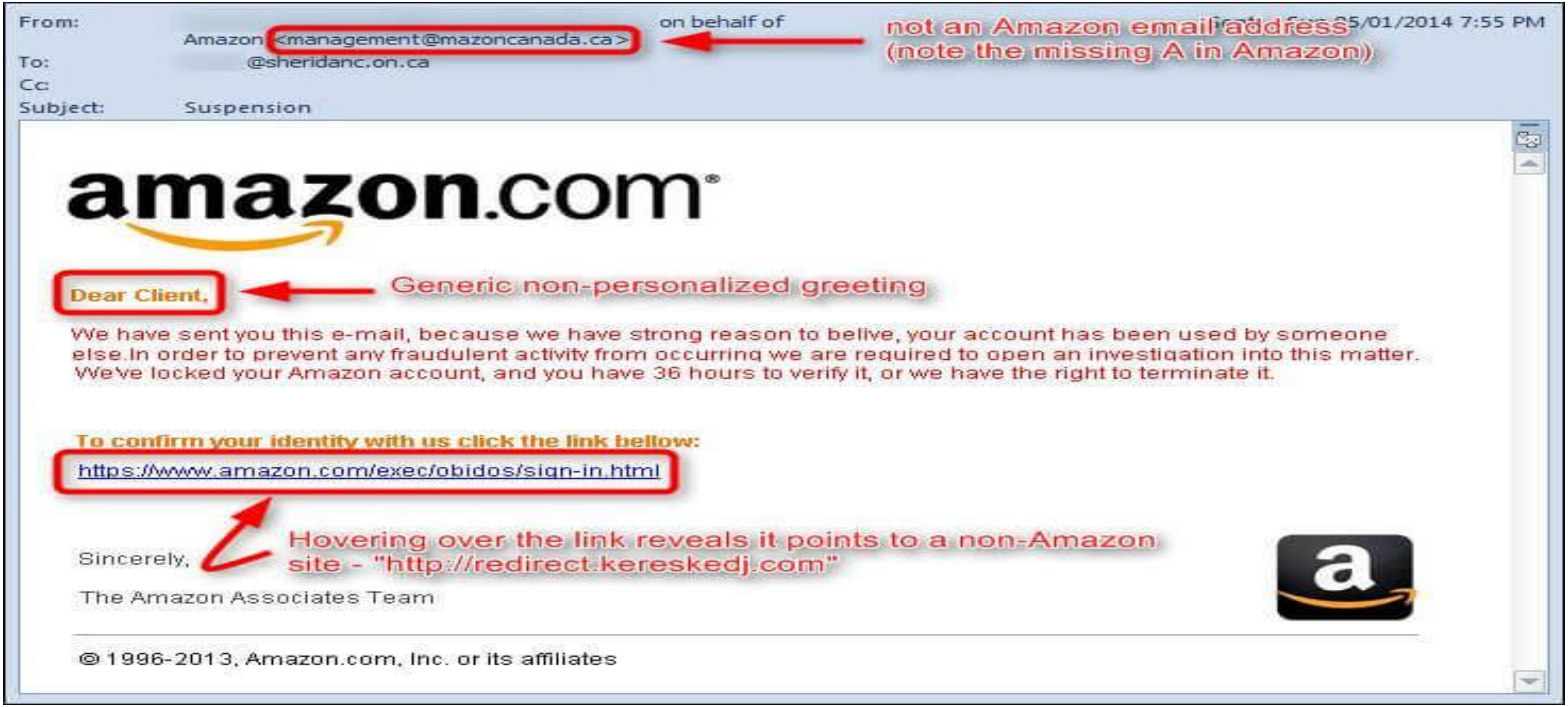


ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

Facts about Social Engineering?

- Everyone is a potential target!
- It’s often easier for cybercriminals to manipulate a human than a computer network or system.
- Attacks can be relatively low-tech, low-cost, and easy to execute.
- Technology is rapidly accelerating along with the sophistication of attacks.
- Most common in Phishing attacks, others include scareware, smishing, pretexting and more

Phishing Email



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>

25/01/2014 7:55 PM

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

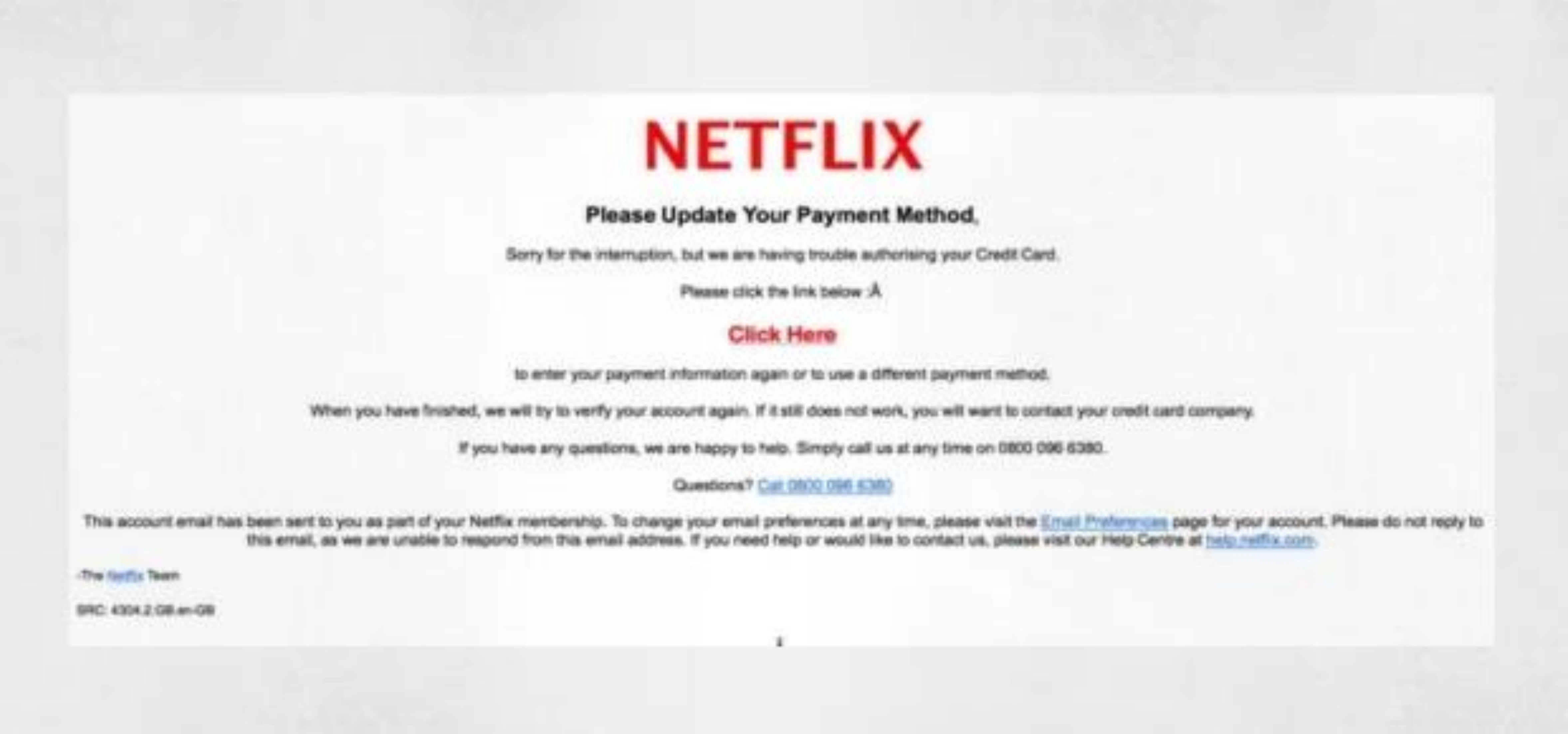
Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Phishing Email



NETFLIX

Please Update Your Payment Method,

Sorry for the interruption, but we are having trouble authorising your Credit Card.

Please click the link below :Â

Click Here

to enter your payment information again or to use a different payment method.

When you have finished, we will try to verify your account again. If it still does not work, you will want to contact your credit card company.

If you have any questions, we are happy to help. Simply call us at any time on 0800 096 6380.

Questions? Call 0800 096 6380

This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the Email Preferences page for your account. Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our Help Centre at help.netflix.com.

-The Netflix Team

SRC: 4304.2.GB.en-GB

ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

How to avoid Phishing Attack?

- Do not respond to communication you are unfamiliar with.
- Do not call any phone numbers listed in an unknown email, text message, or instant message.
- Do not click on any links in an email message and do not open any attachments contained in a suspicious email.
- Watch carefully for attachments, urgency, hyperlink and urgency, can be a problem.. Do not agree on any thing unless you understand as a non suspicious.

- Do not enter personal information in any pop-up screens. Legitimate organizations don’t ask for personal information using pop-up screens. Instead, contact the supposed organization and verify.
- If in doubt, delete the email or message.
- Others?

Common Signs of Phishing

Too Good To Be True

- Eye-catching or attention-grabbing offers designed to attract people’s attention immediately. For instance, a claim that you have won an iPhone, a lottery, or some other prize.

Sense of Urgency

- Act fast because the super deals are only for a limited time.
- Your account will be suspended unless you update your personal details immediately.

Hyperlinks

- Click here to claim your offer.
- Click here to change your login credentials.

Attachments

- Often contain ransomware, malware or other viruses.

TOP 5 Cybersecurity Threats

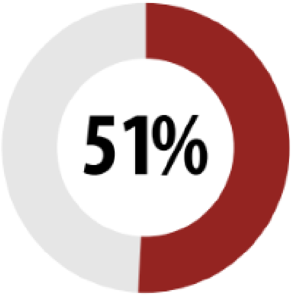
- Social Engineering
- **Ransomware**
- Loss or Theft of Equipment and Data
- Insider, Accidental or Intentional Data Loss
- Attacks against Network Connected Medical Devices

What is Ransomware Attack

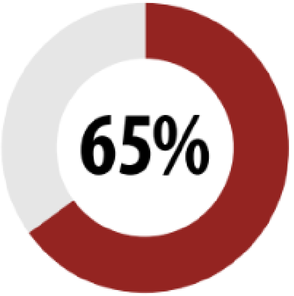
Malicious software (malware) that prevents users from accessing their system or personal files and demands a ransom payment from the user in order to regain access.

Ransomware Threats

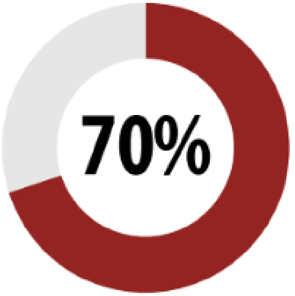
Ransomware Impacts on Patient Safety



of surveyed healthcare organizations reported an increase in breaches and leaks since 2019



reported an increase in the number of patients being diverted to other facilities



reported longer lengths of stays in hospital, delays in procedures and tests and an increase in patient mortality

Expert-level support and a vendor-agnostic, holistic approach to increase visibility and improve cybersecurity ROI.

Ransomware Attack Explanation

- **Description**

– Hackers gain control of data on a computer system and hold it hostage until a ransom is paid.

– Appears to come from a legitimate source through social engineering

– Includes active link or file looks very real.

– This will cause the HIMS fully or partially rendering it in-operational

- **Real-World Scenario**

– Employees receive an email from a credit card company.

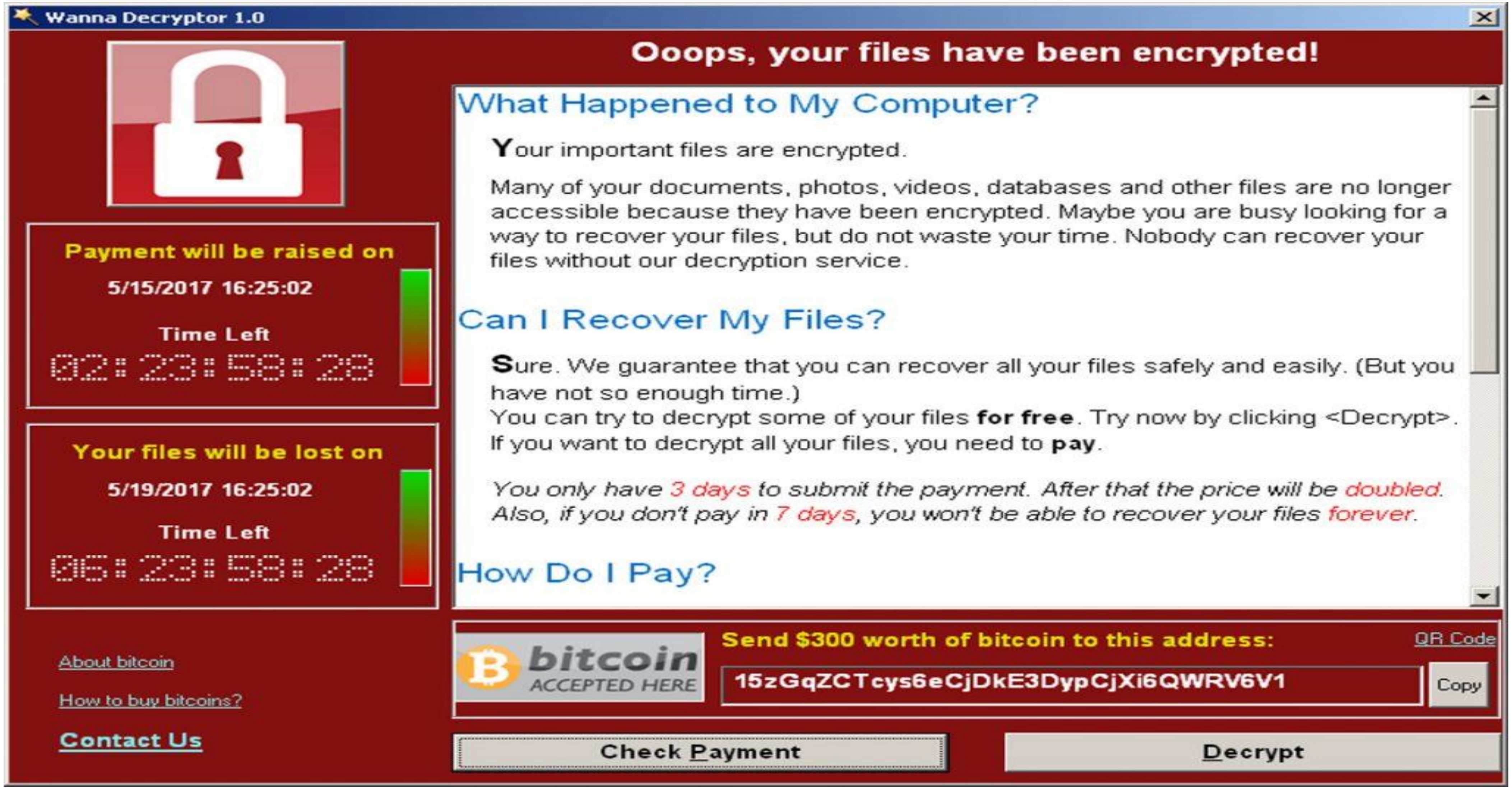
– Email instructs employees to a fake website and is tricked into downloading a security data.

– This security data is a malicious program that request ransom to unlock or unencrypt the data.

- **Impact**

– This attack can put patients in danger and prevent you from delivery in a timely fashion.

Ransomware- More ….



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

*You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.*

How Do I Pay?

Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Ransomware attacks on hospitals on an increase

- One source: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed
- ACTIVELY monitor healthcare cyberattacks. e.g.,
  - https://www.cisa.gov/news-events/cybersecurity-advisories?search_api_fulltext=healthcare&sort_by=field_release_date
  - https://www.aha.org/aha-search?search_api_fulltext=ransomware
- Resource: just released US CISA #StopRansomware Guide
  - https://www.cisa.gov/news-events/alerts/2023/10/19/cisa-nsa-fbi-and-ms-isac-release-update-stopransomware-guide

Important sites, full of information about Ransomware attacks

ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

TOP 5 Cybersecurity Threats

- Social Engineering
- Ransomware
- **Loss or Theft of Equipment and Data**
- Insider, Accidental or Intentional Data Loss
- Attacks against Network Connected Medical Devices

Loss or Theft of Equipment and Data

One laptop is stolen every 53 seconds

70 million smartphones are lost each year

4.3% of company-issued smartphones are lost or stolen every year

80% of the cost of a lost laptops is from data breach

52% of devices are stolen from workplace!

Source: Komando security.com

Loss or Theft of Equipment and Data

Loss or malicious use of data may result in business disruption and compromises patient safety, and may require notification to patients, applicable regulatory agencies, and/or the media.

Data loss through unauthorized access to a system

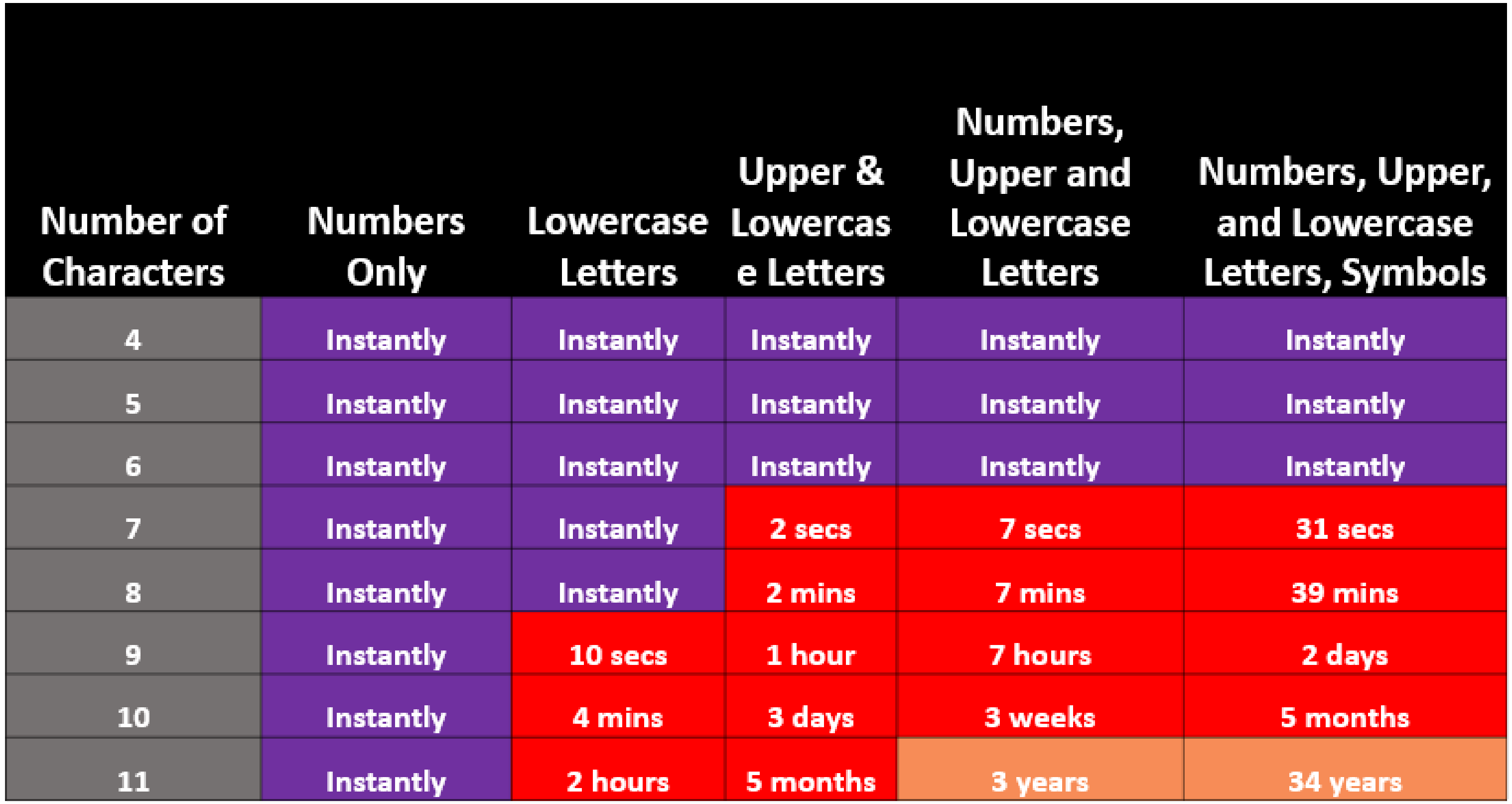
- Not using proper password policy
- Sharing passwords
- Accessing personal or unauthorized non-work internet sites on work computers

Loss or Theft of Equipment and Data

HHS 405(d)
Knowledge on Demand

The time it takes a hacker to break your password!

Data Loss
How strong is your Password?



Number of Characters	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper, and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years

Source: Komando Security.com

Loss or Theft of Equipment and Data

Data loss through USB (Universal Serial Bus) Drives

Safety measures:

- ✓Do not plug an unknown USB drive into your computer
- ✓Be sure to use passwords and encryption if you do you a USB Drive and make sure that you have the information backed up
- ✓Keep personal and business USB Drives separate
- ✓Keep your computer software up to date
- ✓Verify if you have security software on your computer
- ✓Disable “Autorun” on your computer

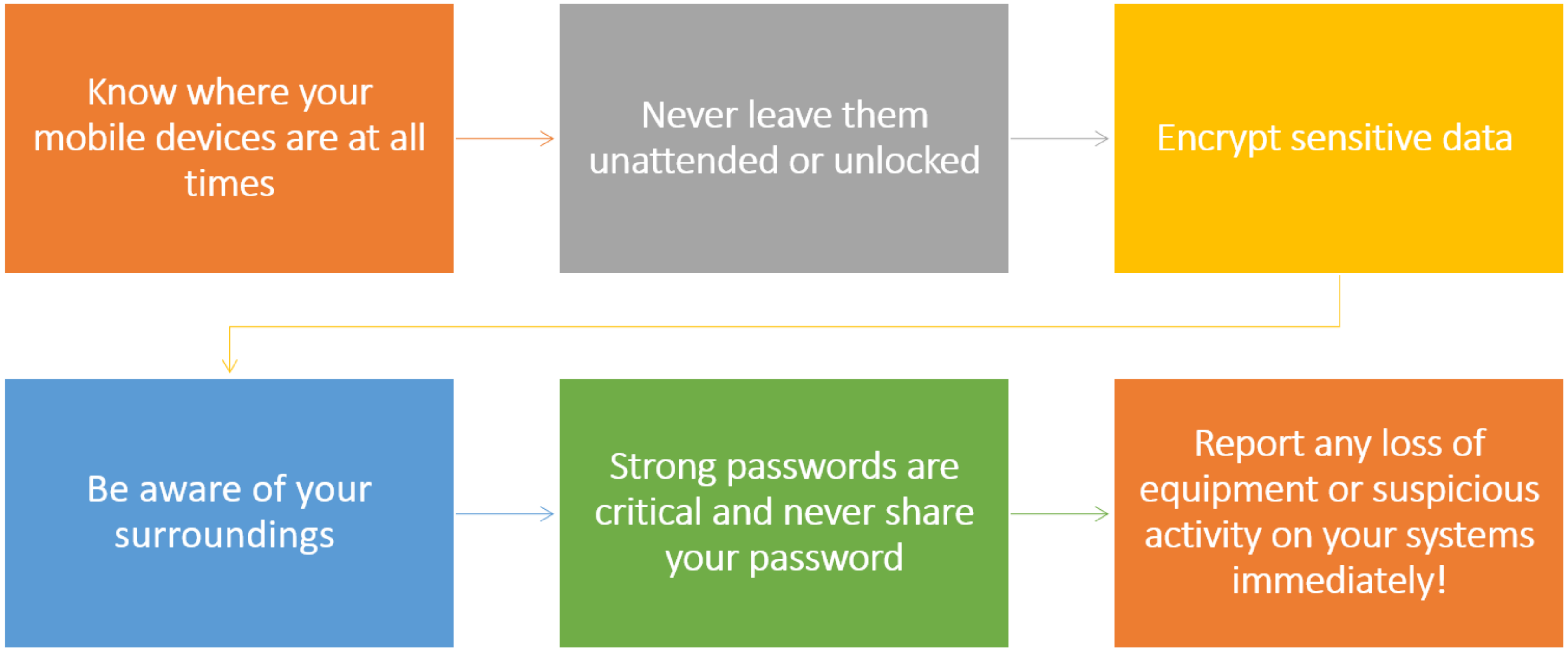
Loss or Theft of Equipment and Data

Know your organization’s policy on removing equipment from the workplace

- Can I travel with my equipment?
- Can I work remotely/offsite and how do I access sensitive information?
- Do I know how to encrypt sensitive data?
- How can I use a secure VPN (virtual private network) and secure password-protected WI-FI?

Loss or Theft of Equipment and Data

Best Practices
How can you protect your devices and data?



Know where your mobile devices are at all times

Never leave them unattended or unlocked

Encrypt sensitive data

Be aware of your surroundings

Strong passwords are critical and never share your password

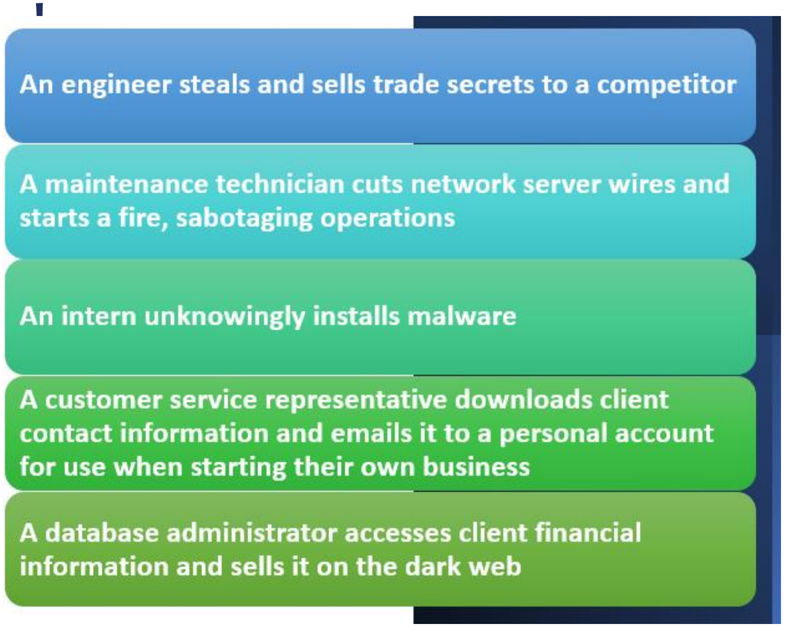
Report any loss of equipment or suspicious activity on your systems immediately!

TOP 5 Cybersecurity Threats

- Social Engineering
- Ransomware
- Loss or Theft of Equipment and Data
- **Insider, Accidental or Intentional Data Loss**
- Attacks against Network Connected Medical Devices

Insider, Accidental or Intentional Data Loss

- Insiders: Employees, contractors or other users who have legitimate access to your computer system and netw
- Accidental Insider Threat
  - Honest mistake
  - Perhaps tricked by a phishing email
  - Procedural errors
  - Negligence
- Intentional Insider threat
- Malicious loss or theft with an objective of personal gain or inflicting harm to a person or the organization



An engineer steals and sells trade secrets to a competitor

A maintenance technician cuts network server wires and starts a fire, sabotaging operations

An intern unknowingly installs malware

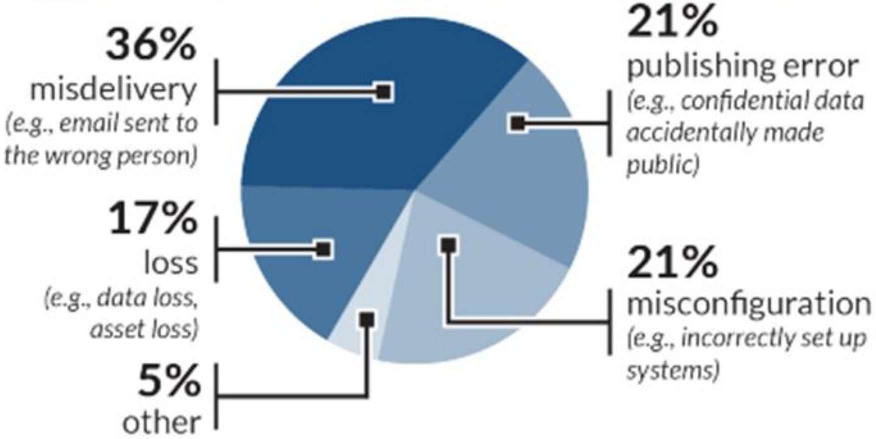
A customer service representative downloads client contact information and emails it to a personal account for use when starting their own business

A database administrator accesses client financial information and sells it on the dark web

Insider, Accidental or Intentional Data Loss

- 61 % of data breaches involving an insider are primarily unintentional causes by negligent insiders
- Lack of awareness of security policies and training
- Leaving an unencrypted mobile device or laptop containing sensitive data unattended
- Employee grievance against the organization

Figure 10. Error varieties in healthcare breaches[12]



Insider, Accidental or Intentional Data loss/ Tips and safety measures

Quick Tips and Safety measures:

✓Employee and vendor screening to make sure that those gaining access are who they are and truly require access

✓Limit access to those who require it based on roles and responsibility

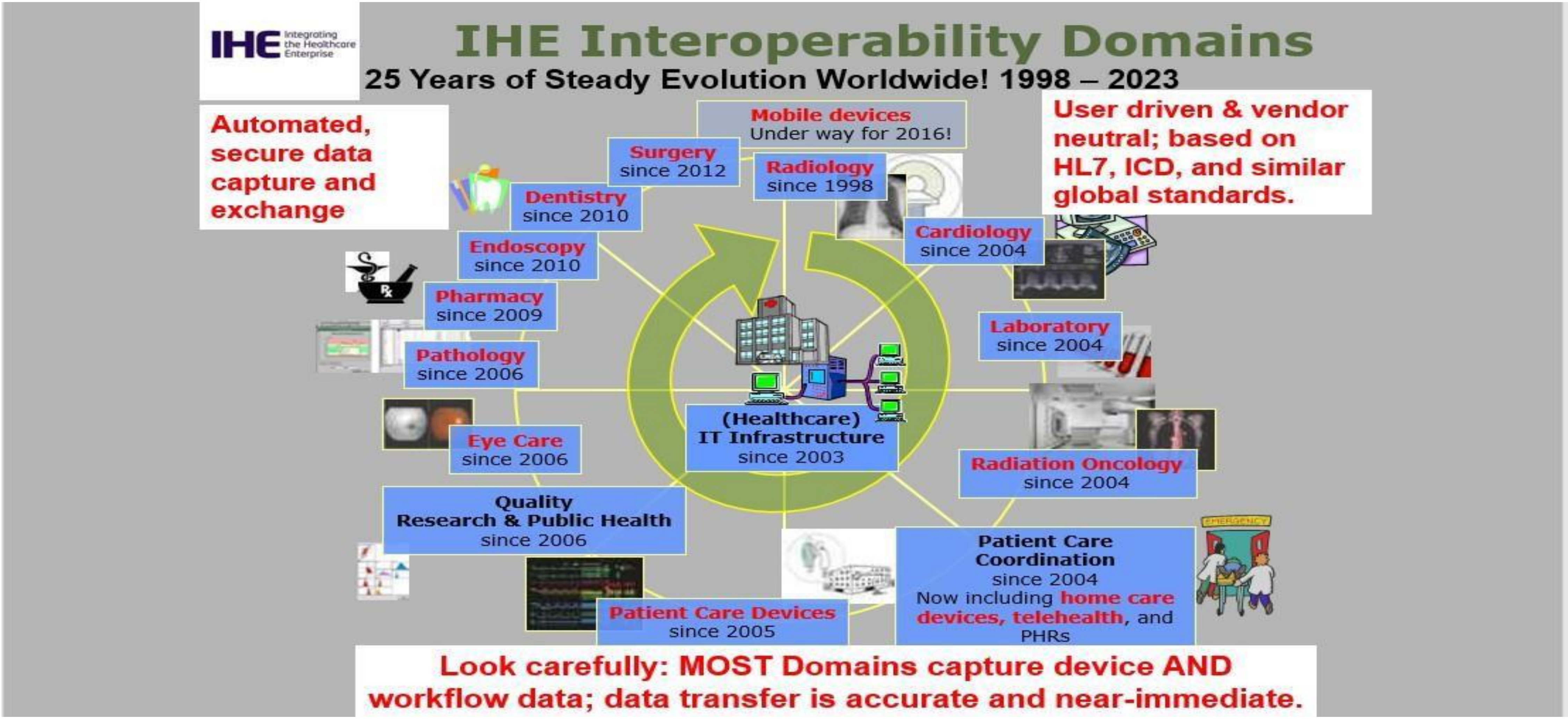
✓Conduct regular security training sessions

✓If you made a mistake or believe you may be a victim of data loss report it to your manager and/or IT /administrator

TOP 5 Cybersecurity Threats

- Social Engineering
- Ransomware
- Loss or Theft of Equipment and Data
- Insider, Accidental or Intentional Data Loss
- **Attacks against Network Connected Medical Devices**

Many devices now can communicate with others ,,



IHE Integrating the Healthcare Enterprise

IHE Interoperability Domains

25 Years of Steady Evolution Worldwide! 1998 – 2023

Automated, secure data capture and exchange

User driven & vendor neutral; based on HL7, ICD, and similar global standards.

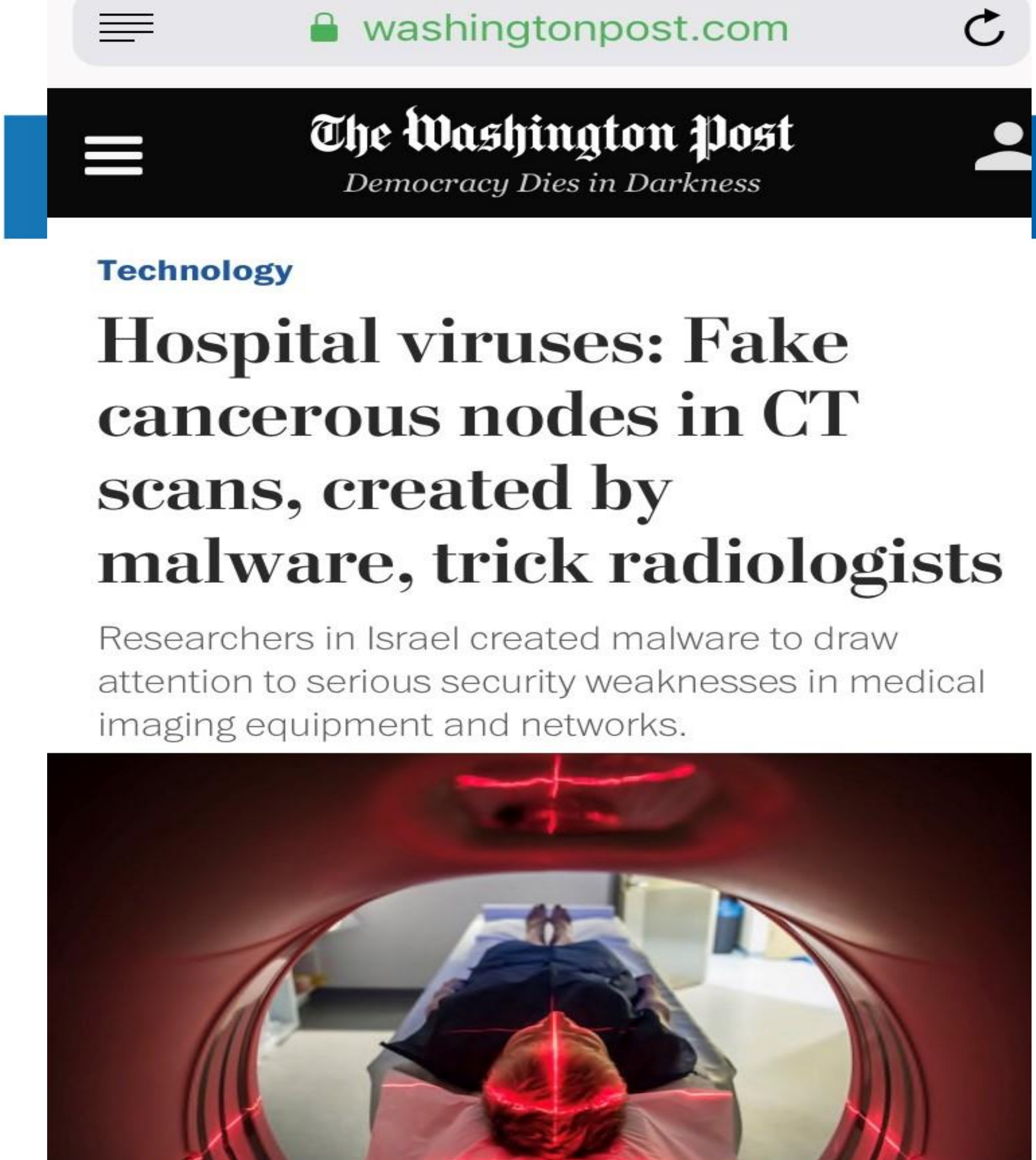
Look carefully: MOST Domains capture device AND workflow data; data transfer is accurate and near-immediate.

Medical devices and Networks

Nowadays, numerous medical devices reside on hospital networks and / or are accessible through wireless networks. These include general devices such as patient monitors, infusion pumps, as well as life-sustaining devices such as ventilators, anesthesia machines and pacemakers

Medical devices altering and manipulation

- Hackers/ Cyber criminals try to tamper with connected medical devices to alter their settings, alter their data and may introduce malicious codes for wrong results.
- Tampered medical devices can lead to patient safety hazards and results in incorrect diagnosis and as such wrong medication and ultimately harm to the patient even may reach death.
- VIPs are at more risk of alteration.



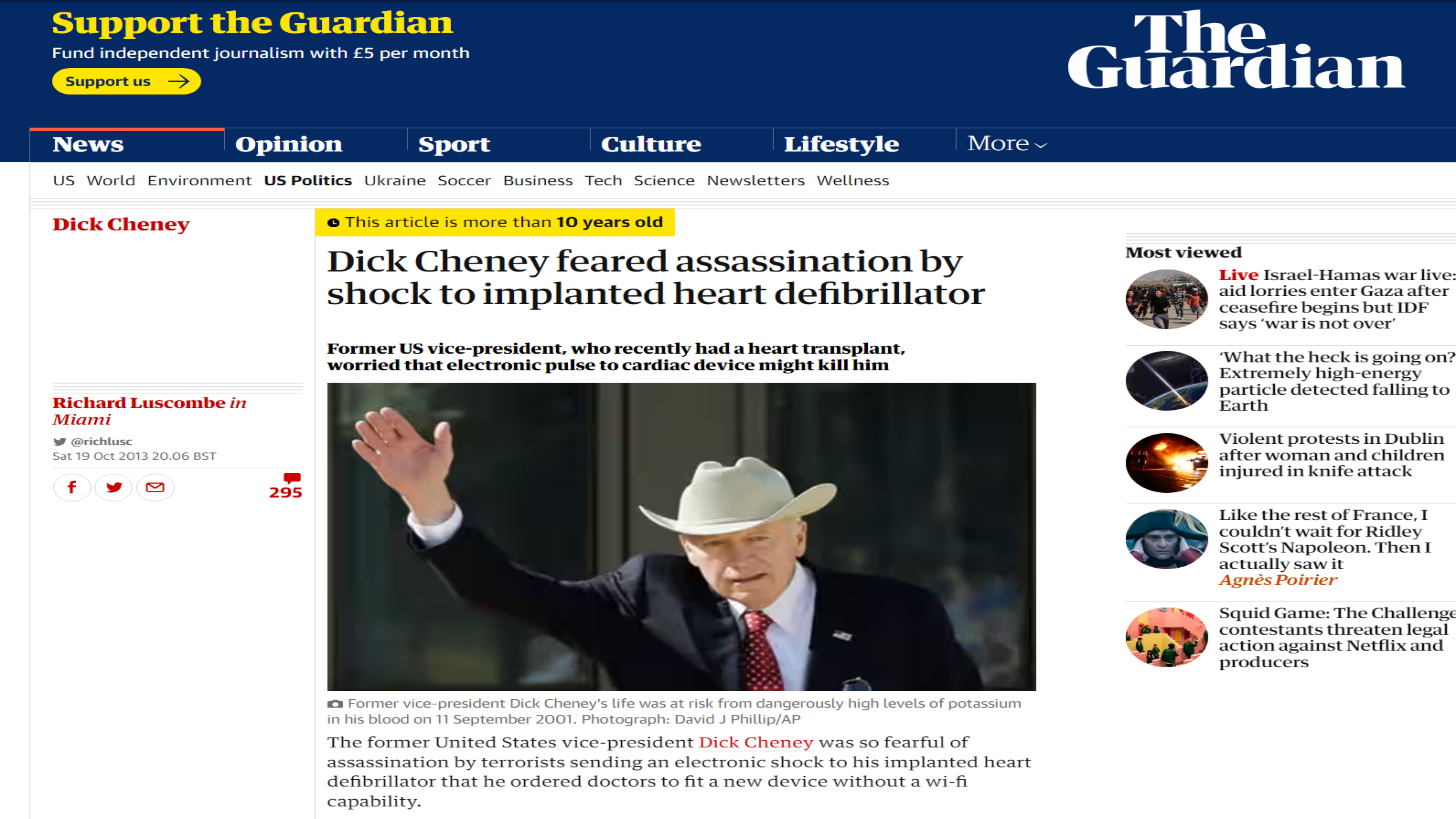
washingtonpost.com

The Washington Post
Democracy Dies in Darkness

Technology

Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists

Researchers in Israel created malware to draw attention to serious security weaknesses in medical imaging equipment and networks.



The Guardian

Dick Cheney

This article is more than **10 years old**

Dick Cheney feared assassination by shock to implanted heart defibrillator

Former US vice-president, who recently had a heart transplant, worried that electronic pulse to cardiac device might kill him

Richard Luscombe *in Miami*

@richlusc

Sat 19 Oct 2013 20.06 BST

295

Former vice-president Dick Cheney's life was at risk from dangerously high levels of potassium in his blood on 11 September 2001. Photograph: David J Phillip/AP

The former United States vice-president Dick Cheney was so fearful of assassination by terrorists sending an electronic shock to his implanted heart defibrillator that he ordered doctors to fit a new device without a wi-fi capability.

Most viewed

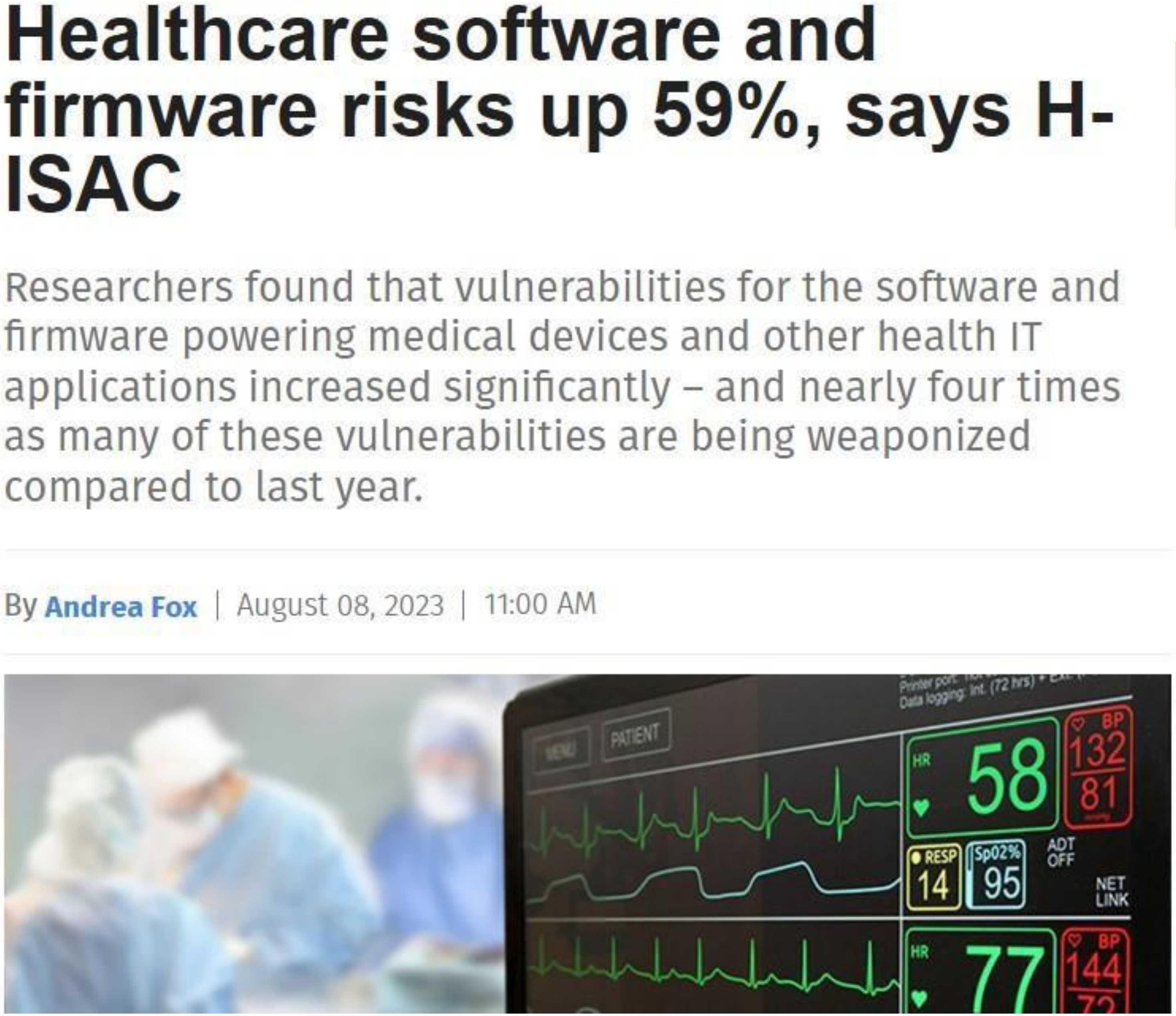
Live Israel-Hamas war live: aid lorries enter Gaza after ceasefire begins but IDF says 'war is not over'

'What the heck is going on? Extremely high-energy particle detected falling to Earth

Violent protests in Dublin after woman and children injured in knife attack

Like the rest of France, I couldn't wait for Ridley Scott's Napoleon. Then I actually saw it *Agnès Poirier*

Squid Game: The Challenge contestants threaten legal action against Netflix and producers



Healthcare software and firmware risks up 59%, says H-ISAC

Researchers found that vulnerabilities for the software and firmware powering medical devices and other health IT applications increased significantly – and nearly four times as many of these vulnerabilities are being weaponized compared to last year.

By **Andrea Fox** | August 08, 2023 | 11:00 AM

See August 2023 overview here:
https://www.healthcareitnews.com/news/healthcare-software-and-firmware-risks-59-says-h-isac

Download full August 2023 report here:
https://h-isac.org/2023-state-of-cybersecurity-for-medical-devices-and-healthcare-systems/

ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

Risks Associated with Networked Medical Devices

- Network-connected/ medical devices disabled by malware for breaching data (IoT)
- Presence of malware on hospital computers, smartphones and tablets, targeting mobile devices that use wireless technology
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical and maintenance personnel) Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)
- Failure to monitor recalls or alerts on medical devices
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals and poor coding/SQL injection.

ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

Threats affecting networked medical devices

1. Hacktivists (anonymous individuals) wishing to cause service interruption and harm
2. Thieves desiring to sell or monetize confidential information, engage in identity theft, commit financial fraud against individuals and/or the health care organization and / or its associates
3. Malicious groups or individuals seeking to cause harm to patients (possibly targeting VIP patients) or seeking to damage the health care organization’s brand.
4. Malware which evades existing antivirus engines and rules but is not specifically targeted at medical devices

US Food and Drug Administration (FDA)

COVER FEATURE

Ensuring Patient Safety in Wireless Medical Device Networks

Vijay Gehlot and Elliot B. Sloane
Villanova University

WMDNs provide many alarms and related clinical data that are life-critical. To avoid

* **Gehlot**, V. and **Sloane**, E.B., Ensuring patient safety in wireless medical device networks, **Computer Magazine**, IEEE, 11(2), 11–17, April 2008

Risk Management of Networked Medical Devices

- Ensure the web-based system (EHR, EMR) works properly
- Coordinate educational sessions for staff to discuss errors and their prevention strategies
- **Ensure software updates are kept up to date**
- Encourage error reporting, to ensure learning from error occurs, and ensure improvement needs are identified.
- Perform an objective self-assessment of the hospital's risk for electronic prescription errors (wrong medication) .
- Share error reduction and prevention strategies and other patient safety information with the other facilities

ARAB bioclinic BIOMEDICAL & CLINICAL ENGINEERING

Recommendations for hospitals

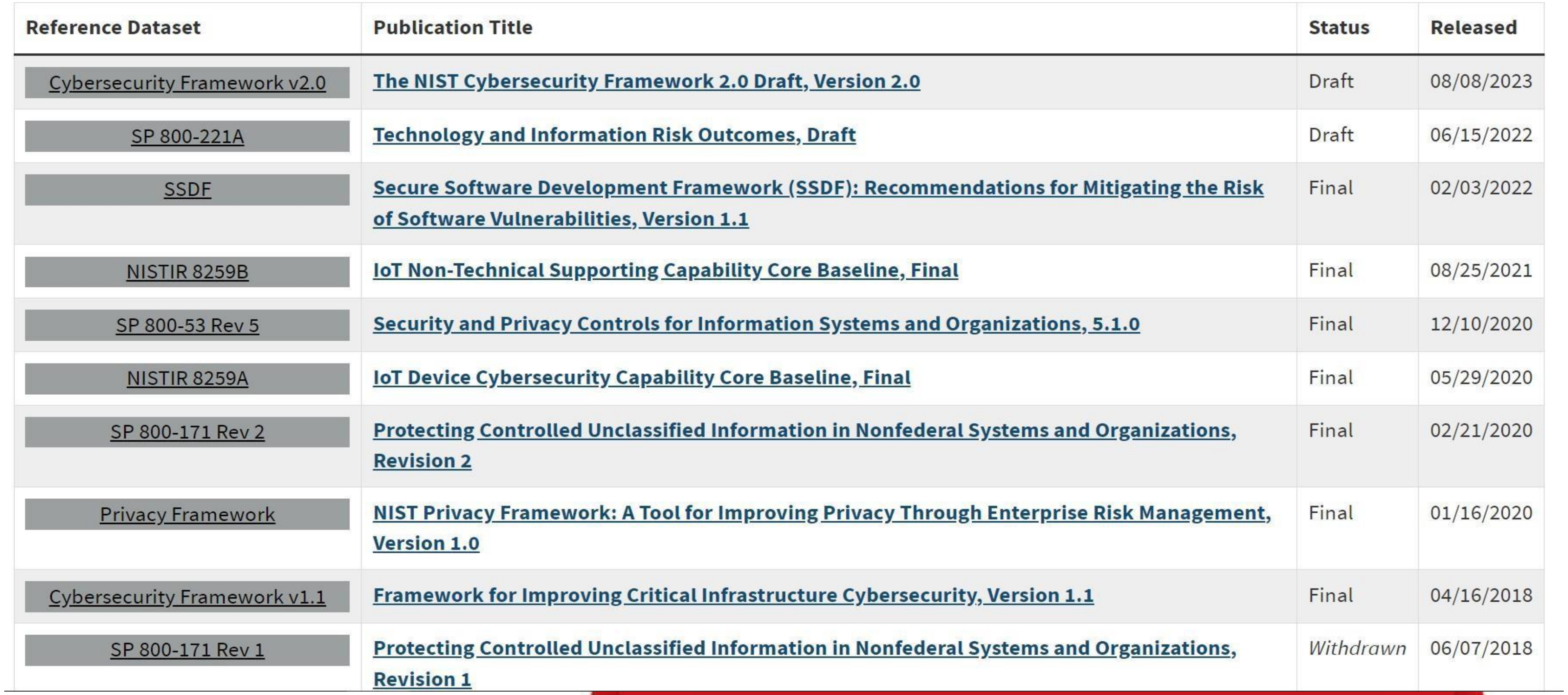
- Establish effective enterprise governance for cyber and information security
- Implement state-of-the-art security measures
- Provide specific IT security requirements for IoT components in the hospital
- Ensure on time software updates
- Establish an information security sharing mechanism
- Conduct risk assessment and vulnerability assessment
- Perform quality audits
- Support multi-stakeholder communication platforms (ISACs)

Take away and lessons learned

- Breaches to health Information security has direct implication to patient safety not only data security
- Know it will happen to you; Plan accordingly
- Plan for two things: 1. to be locked out of records and 2. Unauthorized access of facility records.
- Conduct comprehensive planning; back-ups, plan B, etc.
- Health Information risk management
- Exercise the plan.
- Text less talk more.

Free US Government Cybersecurity Guides

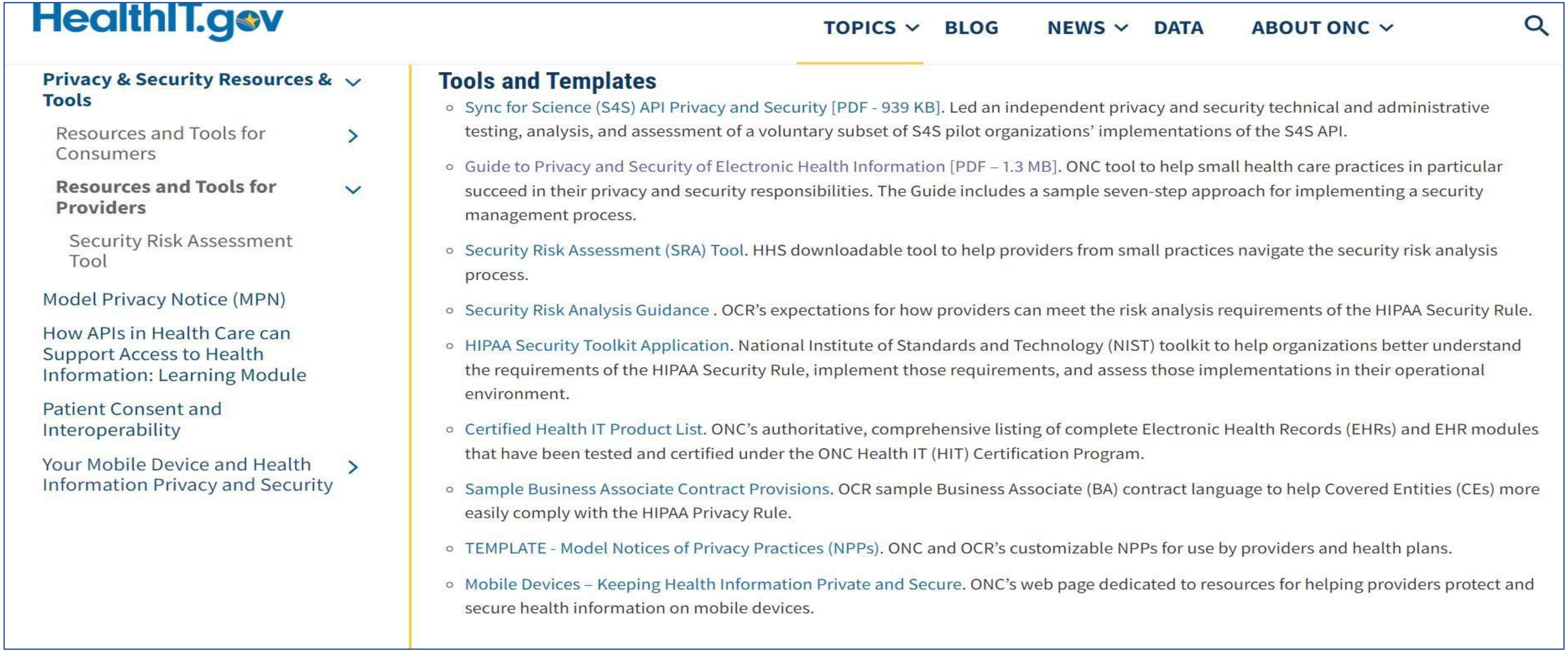
https://csrc.nist.gov/projects/cprt/catalog#/cprt/home



Reference Dataset	Publication Title	Status	Released
Cybersecurity Framework v2.0	The NIST Cybersecurity Framework 2.0 Draft, Version 2.0	Draft	08/08/2023
SP 800-221A	Technology and Information Risk Outcomes, Draft	Draft	06/15/2022
SSDF	Secure Software Development Framework (SSDF): Recommendations for Mitigating the Risk of Software Vulnerabilities, Version 1.1	Final	02/03/2022
NISTIR 8259B	IoT Non-Technical Supporting Capability Core Baseline, Final	Final	08/25/2021
SP 800-53 Rev 5	Security and Privacy Controls for Information Systems and Organizations, 5.1.0	Final	12/10/2020
NISTIR 8259A	IoT Device Cybersecurity Capability Core Baseline, Final	Final	05/29/2020
SP 800-171 Rev 2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Revision 2	Final	02/21/2020
Privacy Framework	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0	Final	01/16/2020
Cybersecurity Framework v1.1	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1	Final	04/16/2018
SP 800-171 Rev 1	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Revision 1	*Withdrawn*	06/07/2018

Additional free materials: US HIPAA

- https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it- privacy-and-security-resources-providers



Privacy & Security Resources & Tools

Resources and Tools for Consumers

Resources and Tools for Providers

Security Risk Assessment Tool

Model Privacy Notice (MPN)

How APIs in Health Care can Support Access to Health Information: Learning Module

Patient Consent and Interoperability

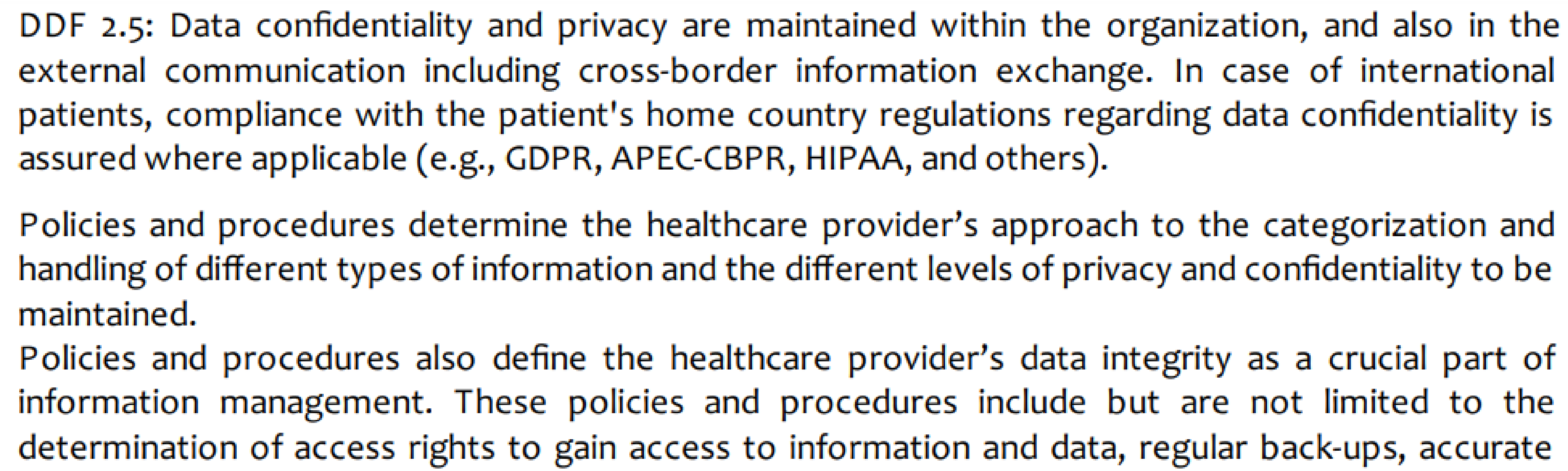
Your Mobile Device and Health Information Privacy and Security

Tools and Templates

- Sync for Science (S4S) API Privacy and Security [PDF - 939 KB]. Led an independent privacy and security technical and administrative testing, analysis, and assessment of a voluntary subset of S4S pilot organizations' implementations of the S4S API.
- Guide to Privacy and Security of Electronic Health Information [PDF – 1.3 MB]. ONC tool to help small health care practices in particular succeed in their privacy and security responsibilities. The Guide includes a sample seven-step approach for implementing a security management process.
- Security Risk Assessment (SRA) Tool. HHS downloadable tool to help providers from small practices navigate the security risk analysis process.
- Security Risk Analysis Guidance . OCR's expectations for how providers can meet the risk analysis requirements of the HIPAA Security Rule.
- HIPAA Security Toolkit Application. National Institute of Standards and Technology (NIST) toolkit to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment.
- Certified Health IT Product List. ONC's authoritative, comprehensive listing of complete Electronic Health Records (EHRs) and EHR modules that have been tested and certified under the ONC Health IT (HIT) Certification Program.
- Sample Business Associate Contract Provisions. OCR sample Business Associate (BA) contract language to help Covered Entities (CEs) more easily comply with the HIPAA Privacy Rule.
- TEMPLATE - Model Notices of Privacy Practices (NPPs). ONC and OCR's customizable NPPs for use by providers and health plans.
- Mobile Devices – Keeping Health Information Private and Secure. ONC's web page dedicated to resources for helping providers protect and secure health information on mobile devices.

Reference to Temos Standards

Chapter 7 – Documentation, Discharge and Follow-Up (DDF)



DDF 2.5: Data confidentiality and privacy are maintained within the organization, and also in the external communication including cross-border information exchange. In case of international patients, compliance with the patient's home country regulations regarding data confidentiality is assured where applicable (e.g., GDPR, APEC-CBPR, HIPAA, and others).

Policies and procedures determine the healthcare provider’s approach to the categorization and handling of different types of information and the different levels of privacy and confidentiality to be maintained.

Policies and procedures also define the healthcare provider’s data integrity as a crucial part of information management. These policies and procedures include but are not limited to the determination of access rights to gain access to information and data, regular back-ups, accurate

ARAB bioclinic
BIOMEDICAL & CLINICAL ENGINEERING

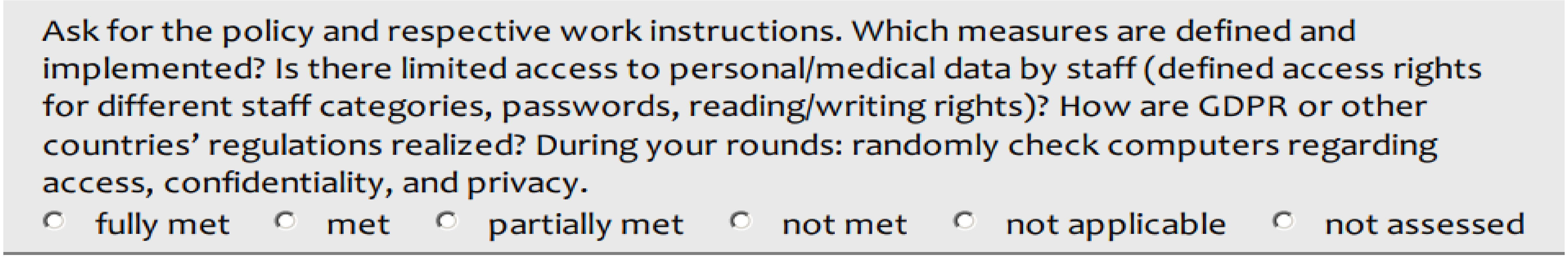
Reference to Temos Standards

Chapter 7 – Docummentation, Discharge and Follow-Up (DDF)

Explanatory note:
GDPR: General Data Protection Regulation of the European Union
APEC-CBPR: Asia-Pacific Economic Cooperation - Cross-Border Privacy Rules
HIPAA: Health Insurance Portability and Accountability Act of the USA

Organizations doing business with European Union (EU) organizations must comply with the "EU General Data Protection Regulation" (GDPR) effective since 25 May 2018.

The GDPR not only applies to organizations located within the EU but it also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the organization's location.

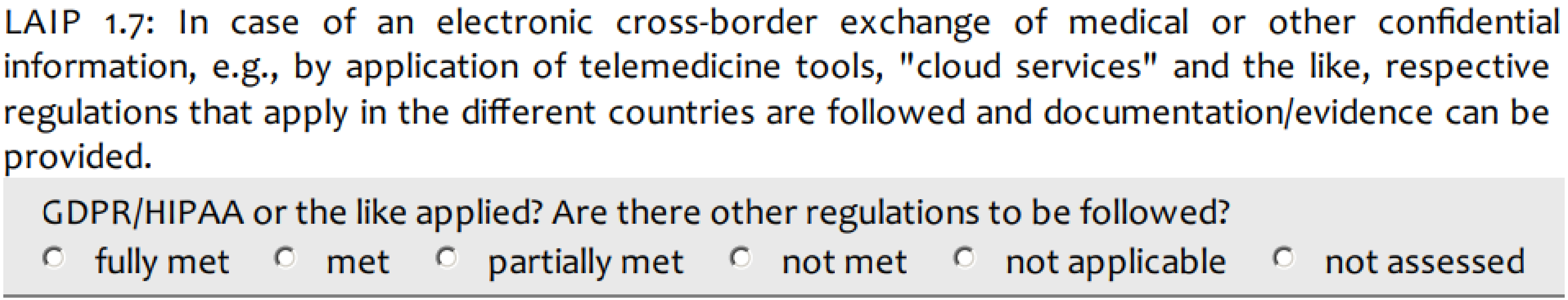


Ask for the policy and respective work instructions. Which measures are defined and implemented? Is there limited access to personal/medical data by staff (defined access rights for different staff categories, passwords, reading/writing rights)? How are GDPR or other countries' regulations realized? During your rounds: randomly check computers regarding access, confidentiality, and privacy.

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

Reference to Temos Standards

Chapter 11 – Legal aspects in International Patient Management (LAIP)



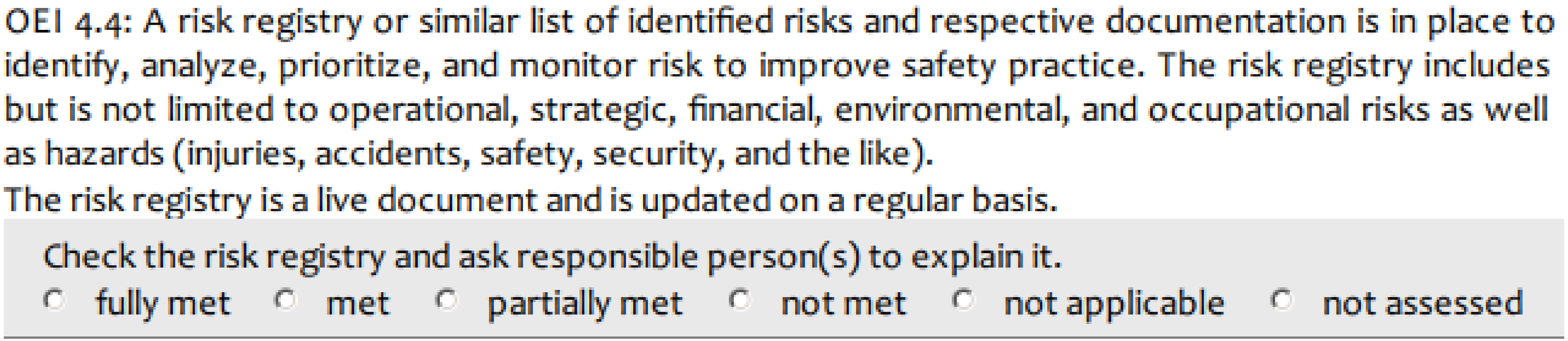
LAIP 1.7: In case of an electronic cross-border exchange of medical or other confidential information, e.g., by application of telemedicine tools, "cloud services" and the like, respective regulations that apply in the different countries are followed and documentation/evidence can be provided.

GDPR/HIPAA or the like applied? Are there other regulations to be followed?

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

Reference to Temos Standards

Chapter 13 – Outcome, effectiveness and quality improvement (OEI)



OEI 4.4: A risk registry or similar list of identified risks and respective documentation is in place to identify, analyze, prioritize, and monitor risk to improve safety practice. The risk registry includes but is not limited to operational, strategic, financial, environmental, and occupational risks as well as hazards (injuries, accidents, safety, security, and the like).

The risk registry is a live document and is updated on a regular basis.

Check the risk registry and ask responsible person(s) to explain it.

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

Reference to Temos Standards

Chapter 18: Facility Services, Infrastructure and Safety (FSIS)

Biomedical/Clinical Engineering Services

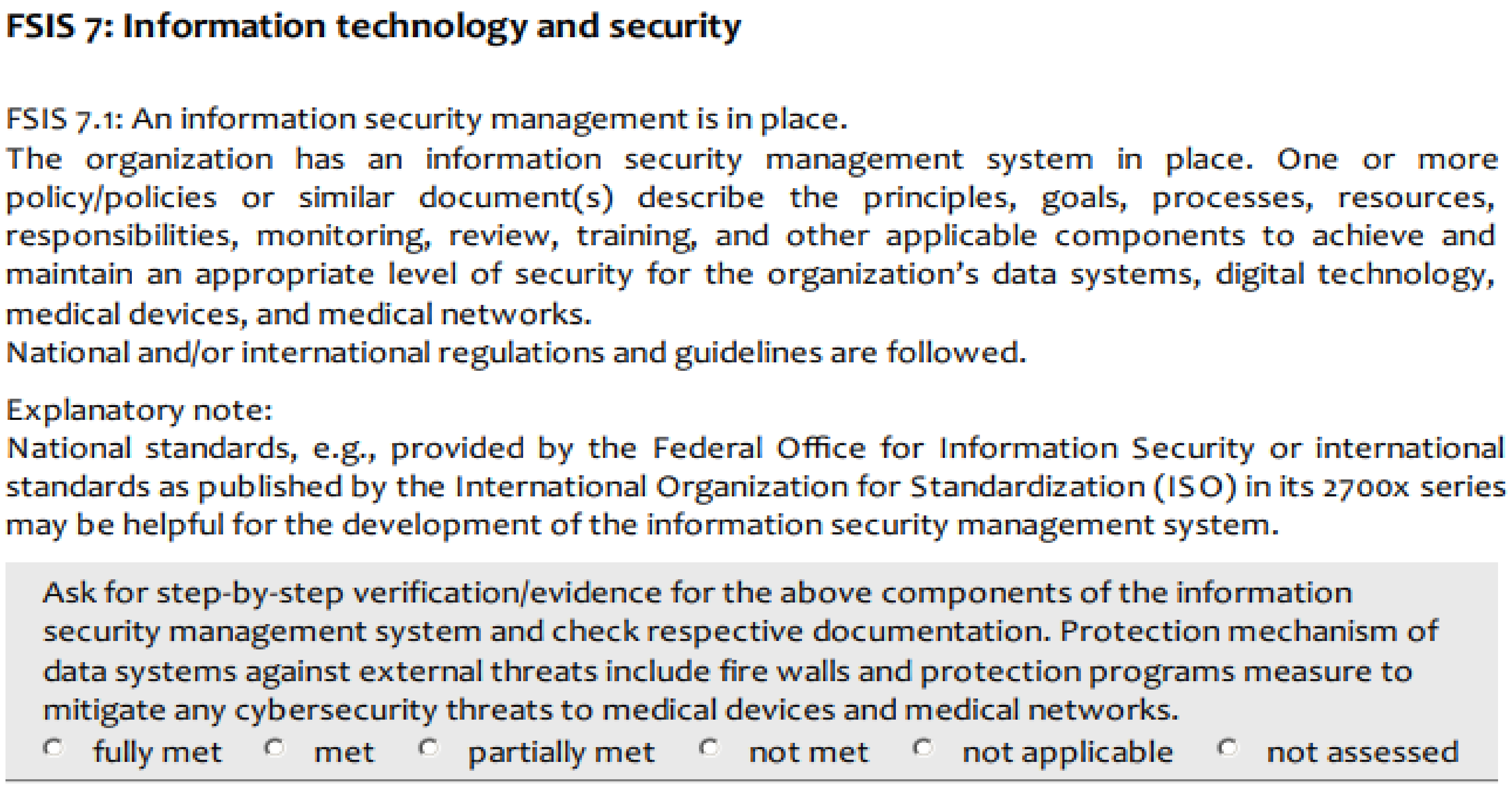
FSIS 5.3: The planning system or work order management involves systematic, measurable and traceable methods to all initial inspections, preventive maintenance, calibration, breakdown, recalls, and repairs

Check the history from purchase and include the services done on such selected equipment. Recall programs and monitoring need to be reviewed. For quality control and post-order work management see also FSIS 5.6

- fully met . partially met . not met . not applicable . not assessed

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS)



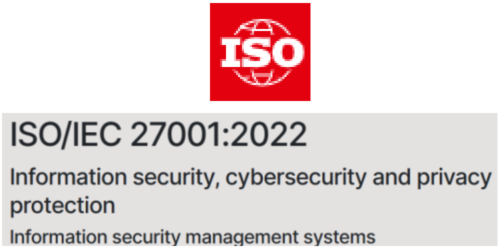
FSIS 7: Information technology and security

FSIS 7.1: An information security management is in place.
The organization has an information security management system in place. One or more policy/policies or similar document(s) describe the principles, goals, processes, resources, responsibilities, monitoring, review, training, and other applicable components to achieve and maintain an appropriate level of security for the organization's data systems, digital technology, medical devices, and medical networks.
National and/or international regulations and guidelines are followed.

Explanatory note:
National standards, e.g., provided by the Federal Office for Information Security or international standards as published by the International Organization for Standardization (ISO) in its 2700x series may be helpful for the development of the information security management system.

Ask for step-by-step verification/evidence for the above components of the information security management system and check respective documentation. Protection mechanism of data systems against external threats include fire walls and protection programs measure to mitigate any cybersecurity threats to medical devices and medical networks.

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed



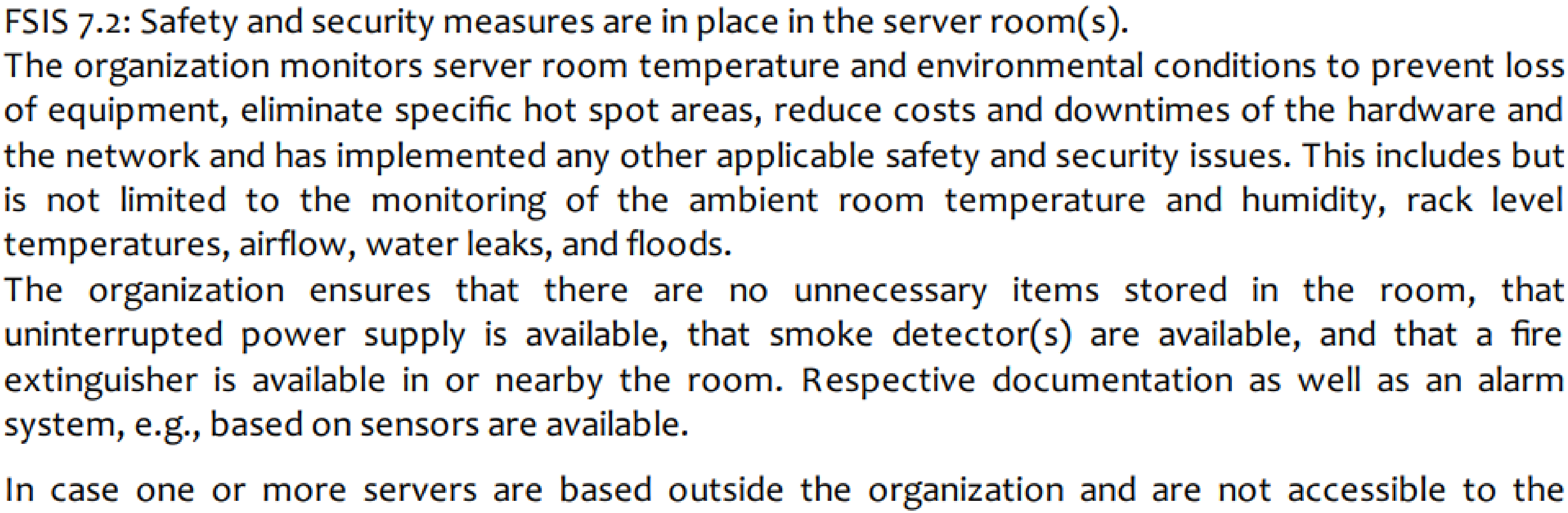
ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection

Information security management systems

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS)



FSIS 7.2: Safety and security measures are in place in the server room(s).

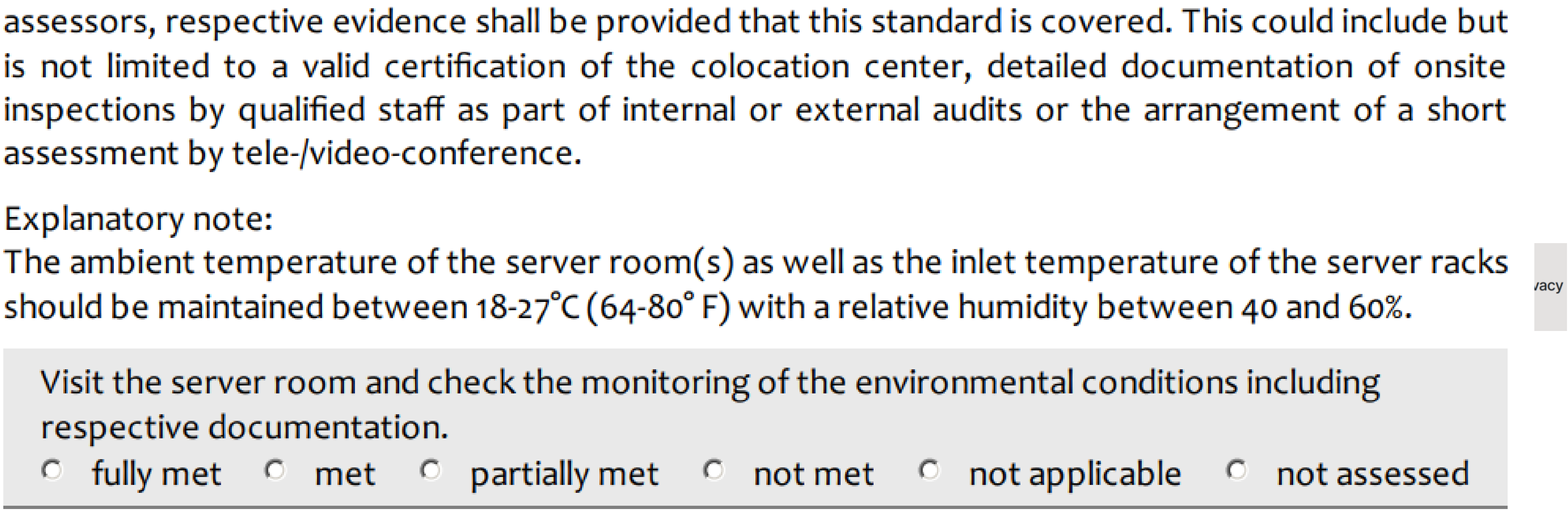
The organization monitors server room temperature and environmental conditions to prevent loss of equipment, eliminate specific hot spot areas, reduce costs and downtimes of the hardware and the network and has implemented any other applicable safety and security issues. This includes but is not limited to the monitoring of the ambient room temperature and humidity, rack level temperatures, airflow, water leaks, and floods.

The organization ensures that there are no unnecessary items stored in the room, that uninterrupted power supply is available, that smoke detector(s) are available, and that a fire extinguisher is available in or nearby the room. Respective documentation as well as an alarm system, e.g., based on sensors are available.

In case one or more servers are based outside the organization and are not accessible to the

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS) continued ....



assessors, respective evidence shall be provided that this standard is covered. This could include but is not limited to a valid certification of the colocation center, detailed documentation of onsite inspections by qualified staff as part of internal or external audits or the arrangement of a short assessment by tele-/video-conference.

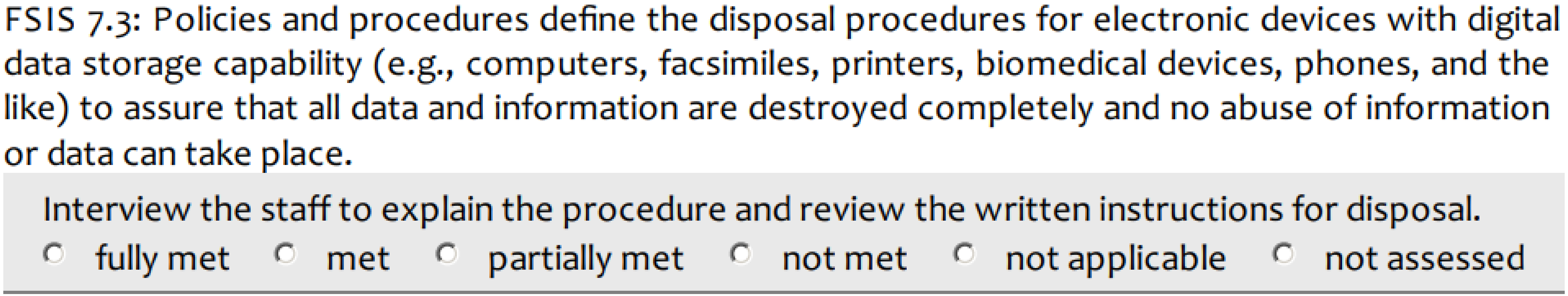
Explanatory note:
The ambient temperature of the server room(s) as well as the inlet temperature of the server racks should be maintained between 18-27°C (64-80° F) with a relative humidity between 40 and 60%.

Visit the server room and check the monitoring of the environmental conditions including respective documentation.

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS) continued ....



FSIS 7.3: Policies and procedures define the disposal procedures for electronic devices with digital data storage capability (e.g., computers, facsimiles, printers, biomedical devices, phones, and the like) to assure that all data and information are destroyed completely and no abuse of information or data can take place.

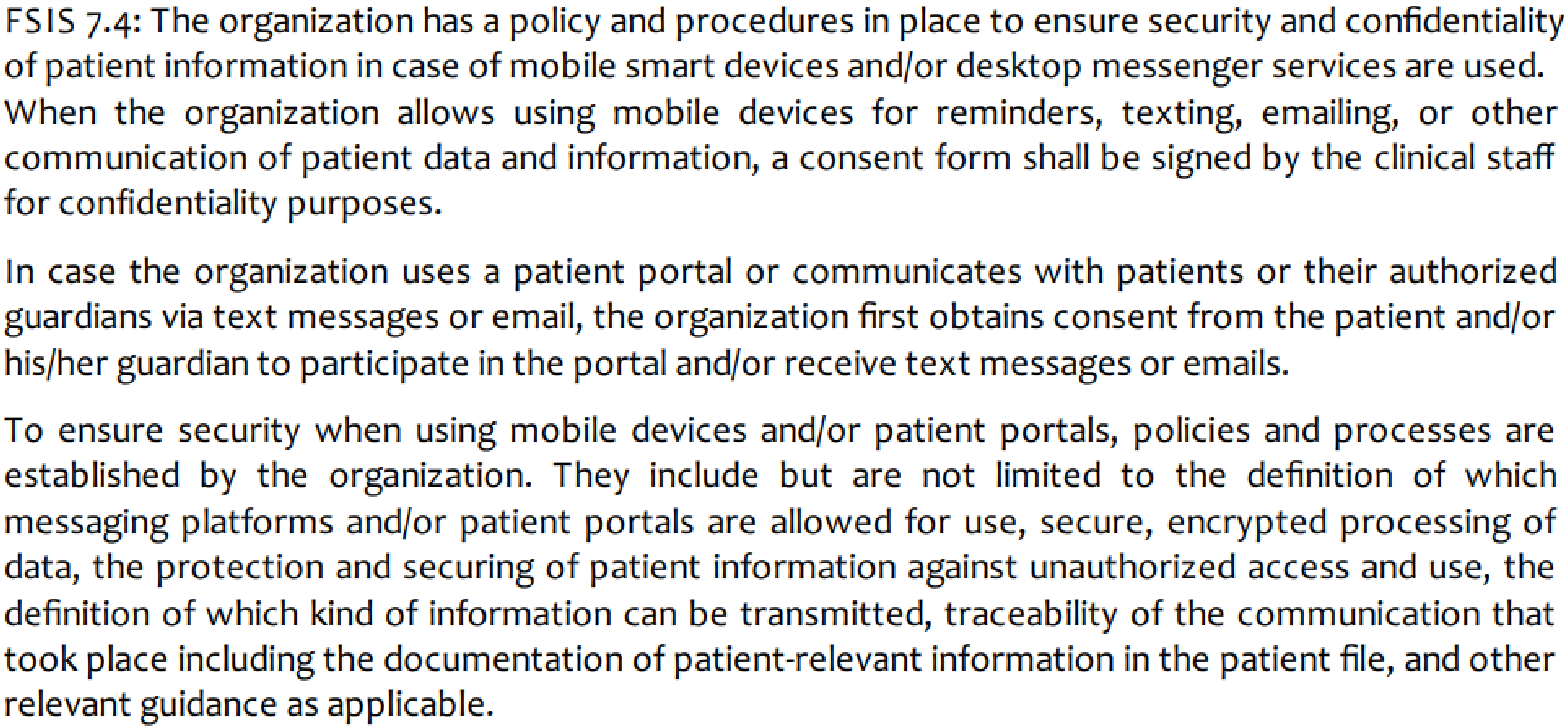
Interview the staff to explain the procedure and review the written instructions for disposal.

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

information security management systems

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS) continued ....



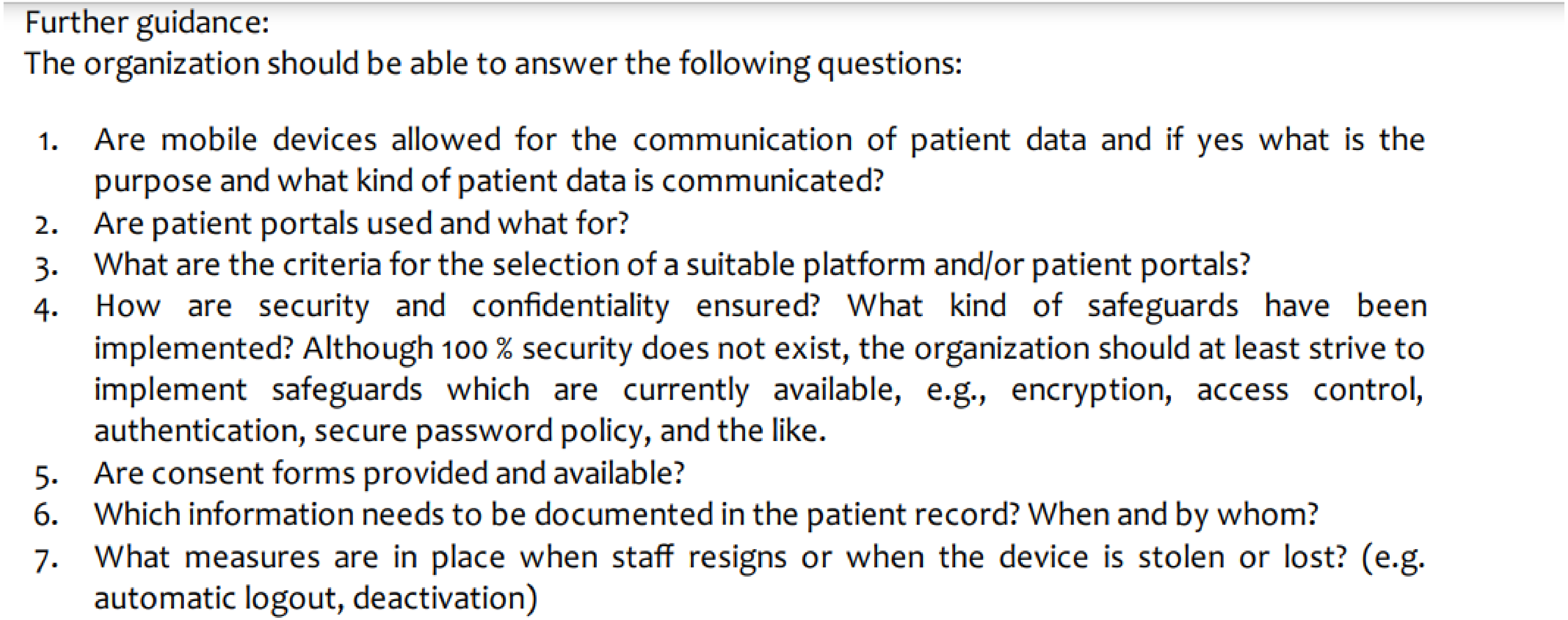
FSIS 7.4: The organization has a policy and procedures in place to ensure security and confidentiality of patient information in case of mobile smart devices and/or desktop messenger services are used. When the organization allows using mobile devices for reminders, texting, emailing, or other communication of patient data and information, a consent form shall be signed by the clinical staff for confidentiality purposes.

In case the organization uses a patient portal or communicates with patients or their authorized guardians via text messages or email, the organization first obtains consent from the patient and/or his/her guardian to participate in the portal and/or receive text messages or emails.

To ensure security when using mobile devices and/or patient portals, policies and processes are established by the organization. They include but are not limited to the definition of which messaging platforms and/or patient portals are allowed for use, secure, encrypted processing of data, the protection and securing of patient information against unauthorized access and use, the definition of which kind of information can be transmitted, traceability of the communication that took place including the documentation of patient-relevant information in the patient file, and other relevant guidance as applicable.

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS) continued ....



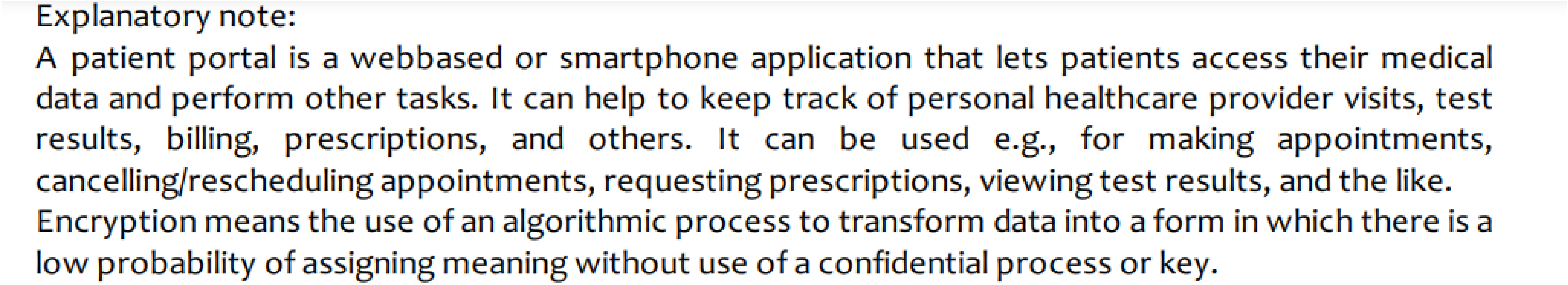
Further guidance:

The organization should be able to answer the following questions:

1. Are mobile devices allowed for the communication of patient data and if yes what is the purpose and what kind of patient data is communicated?
2. Are patient portals used and what for?
3. What are the criteria for the selection of a suitable platform and/or patient portals?
4. How are security and confidentiality ensured? What kind of safeguards have been implemented? Although 100 % security does not exist, the organization should at least strive to implement safeguards which are currently available, e.g., encryption, access control, authentication, secure password policy, and the like.
5. Are consent forms provided and available?
6. Which information needs to be documented in the patient record? When and by whom?
7. What measures are in place when staff resigns or when the device is stolen or lost? (e.g. automatic logout, deactivation)

Reference to Temos Standards

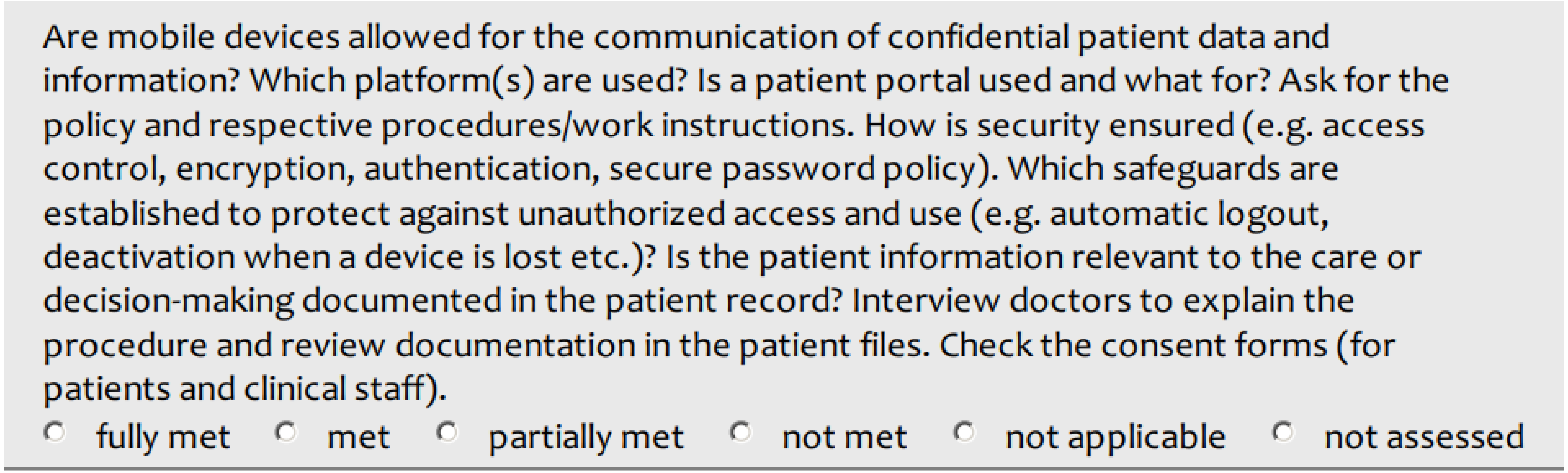
Chapter 18 – Facility Services, Infrastructure and Safety (FSIS) continued ....



Explanatory note:

A patient portal is a webbased or smartphone application that lets patients access their medical data and perform other tasks. It can help to keep track of personal healthcare provider visits, test results, billing, prescriptions, and others. It can be used e.g., for making appointments, cancelling/rescheduling appointments, requesting prescriptions, viewing test results, and the like.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

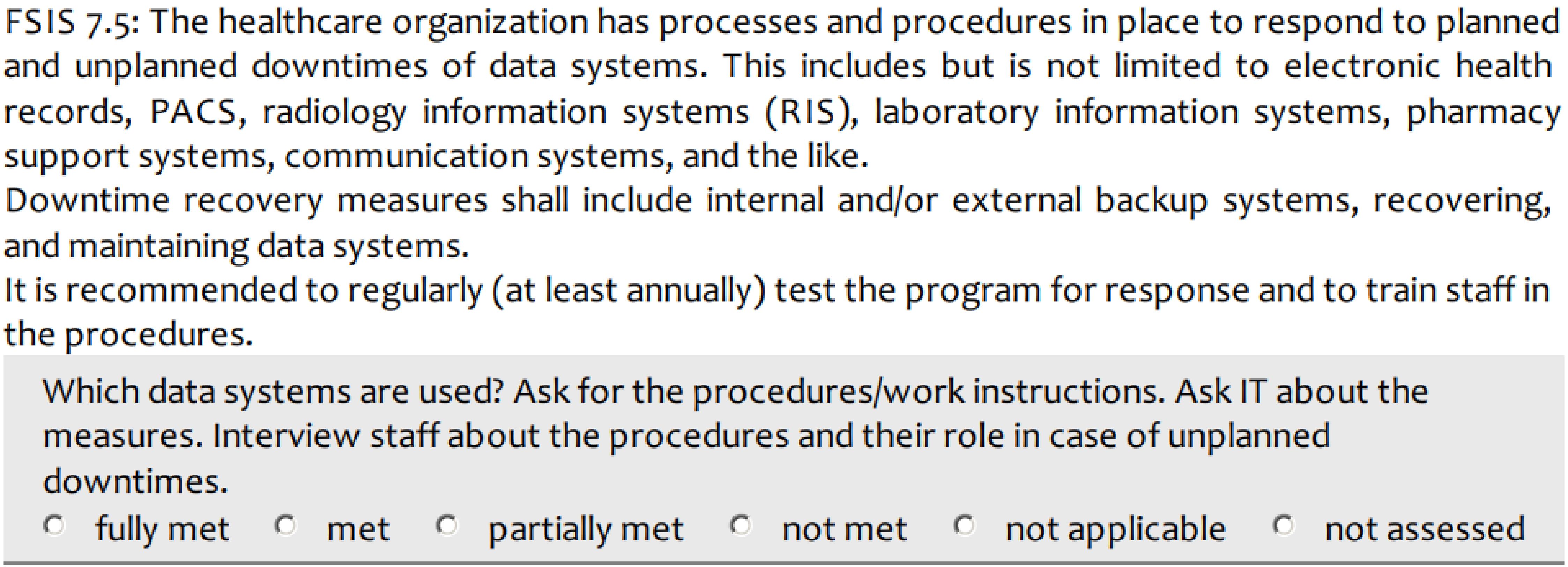


Are mobile devices allowed for the communication of confidential patient data and information? Which platform(s) are used? Is a patient portal used and what for? Ask for the policy and respective procedures/work instructions. How is security ensured (e.g. access control, encryption, authentication, secure password policy). Which safeguards are established to protect against unauthorized access and use (e.g. automatic logout, deactivation when a device is lost etc.)? Is the patient information relevant to the care or decision-making documented in the patient record? Interview doctors to explain the procedure and review documentation in the patient files. Check the consent forms (for patients and clinical staff).

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

Reference to Temos Standards

Chapter 18 – Facility Services, Infrastructure and Safety (FSIS) continued ....



FSIS 7.5: The healthcare organization has processes and procedures in place to respond to planned and unplanned downtimes of data systems. This includes but is not limited to electronic health records, PACS, radiology information systems (RIS), laboratory information systems, pharmacy support systems, communication systems, and the like.

Downtime recovery measures shall include internal and/or external backup systems, recovering, and maintaining data systems.

It is recommended to regularly (at least annually) test the program for response and to train staff in the procedures.

Which data systems are used? Ask for the procedures/work instructions. Ask IT about the measures. Interview staff about the procedures and their role in case of unplanned downtimes.

○ fully met ○ met ○ partially met ○ not met ○ not applicable ○ not assessed

References

- 405(d) :: Top 5 Threats (hhs.gov)
- About ENISA - The European Union Agency for Cybersecurity — ENISA (europa.eu)
- BSI - Federal Office for Information Security (bund.de)
- ISO - International Organization for Standardization
- **Alarming Cyber Security Facts and Stats. Cybint Cyber Solutions. 3 Dec. 2018.** https://www.cybintsolutions.com/cyber-security-facts-stats/
- **Social Engineering. Imperva Incapsula. 2 Mar. 2019.** https://www.incapsula.com/web-application-security/social-engineering-attack.html
- **Three Scary Social Engineering Facts. Proofpoint. 31 Oct. 2016.** https://www.wombatsecurity.com/blog/three-scary-social-engineering-facts : https://www.aha.org/center/cybersecurity-and-risk- advisory-services/ransomware-attacks-hospitals-have-changed
- https://www.cisa.gov/news-events/alerts/2023/10/19/cisa-nsa-fbi-and-ms-isac- release-update-stopransomware-guidehttps://csrc.nist.gov/CSRC/media/Events/HIPAA-2010-Safeguarding-Health-Information-Buil/documents/1-4-

ARAB bioclinic

BIOMEDICAL & CLINICAL ENGINEERING

BIOMEDICAL & CLINICAL ENGINEERING

THANK YOU!

Within the 21st International Operations
& Maintenance Conference in the Arab Countries

An Initiative by

OMAINTEC
المجلس العربي للتشغيل والصيانة
Arab Operations & Maintenance Council

Organized by

EXICON. International Group
مجموعة أكزيكون الدولية

Collaborators

الجمعية العلمية السعودية للهندسة الطبية

Biomed Engineering EGYPT