



CIBERSECURITY MANUAL FOR NURCES

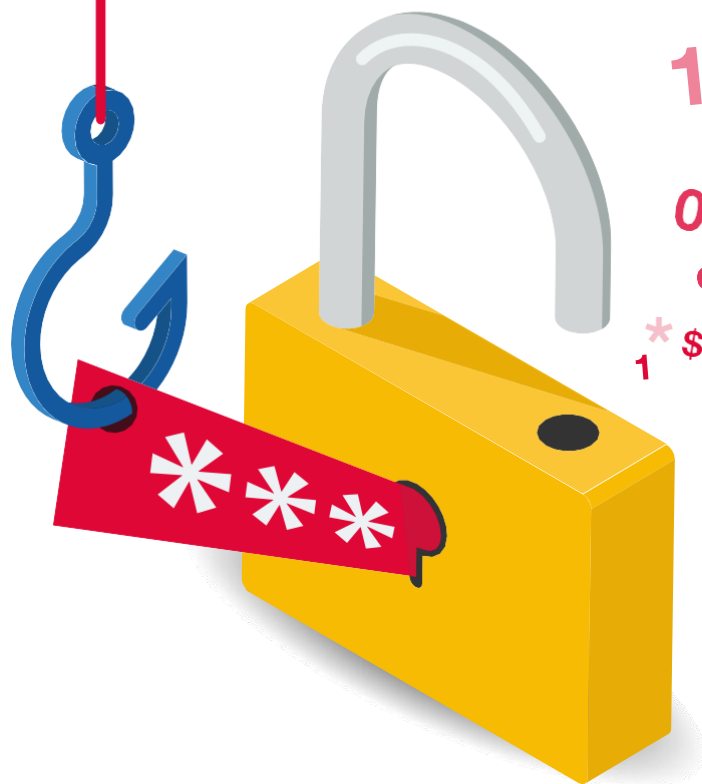


INTRODUCTION

Did you know that healthcare is one of the most attractive sectors for hackers? In addition to health data being more sensitive and profitable than banking data on the dark web (as they include permanent identification data such as the healthcare user number), it is also the most vulnerable sector to attacks.

Just as better and more efficient care for our public requires hygiene habits and procedures from healthcare professionals, cyber hygiene habits are also essential!





WHAT ARE THE RISKS?

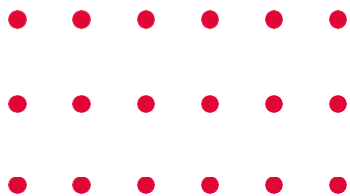
- Dissemination of information via medication carts or open/shared consultation rooms ;
- Unlocked computers in service areas (consultation rooms);
- Sharing the same access credentials among colleagues;
- Clicking on links from questionable sources.

Safeguarding the patient's personal data and preventing exposure to unauthorized access is our duty. The patient's safety also depends on information and cybersecurity!

Over the years, there has been a considerable increase in cyberattacks targeting the healthcare sector. The most common method of attack is via email, through phishing (theft of information) or ransomware (a type of attack that prevents access to data, systems, or devices until the demanded ransom is paid).

In 2016, in the United States, a ransomware attack on the Hollywood Presbyterian Medical Center shut down the network for 10 days, preventing staff from accessing medical records or using medical equipment until the ransom was paid.

Similarly, in 2017, in the United Kingdom, the WannaCry virus cost the NHS (National Health System) £92 million and led to the cancellation of 1,900 treatments and the redirection of patients.



HOW TO ACT?

JUST LIKE...

When starting a shift, we change shoes, put on a coat, and pick up work materials.

WE MUST ALSO...

Ensure that no personal devices, such as USB drives or mobile phones, are connected to the work computers or the organization's networks.



JUST LIKE...

We close the curtain to protect the patient's privacy.

WE MUST ALSO...

Minimize windows or tabs containing patient information and lock computers, even during short absences.



JUST LIKE...

We welcome the patients and carefully analyze their symptoms.

WE MUST ALSO...

Read each email carefully and always be suspicious when it has malicious origins or objectives.



JUST LIKE...

We support and ensure that operations are successfully completed.

WE MUST ALSO...

Understand that when sharing a work computer, we must always log out after using the system.

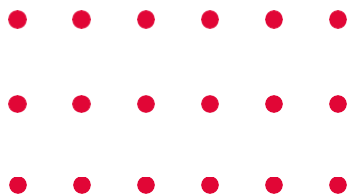
JUST LIKE...

We do not use the same dressing materials already used for different patients.

WE MUST ALSO...

Use only our own access credentials for systems and never those of colleagues.



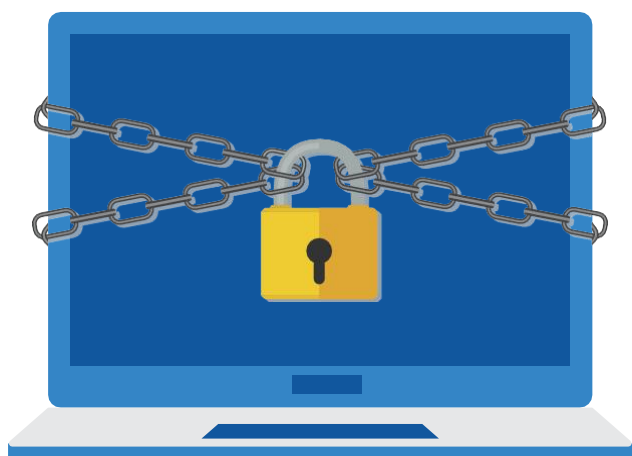


JUST LIKE...

We contact the assigned doctor when in doubt.

WE MUST ALSO...

Contact the IT Department if we have any questions related to information security or need to report an incident.



JUST LIKE...

We clean and disinfect wounds and apply dressings to prevent contamination from external bacteria.

WE MUST ALSO...

Be alert to potential anomalies in antivirus and firewall systems and report them to the IT Department when detected.



JUST LIKE...

During shift handovers, we share clinical information with colleagues in a private space.

WE MUST ALSO...

Ensure that digitally shared information is transmitted securely and that only the intended recipients have access.



10 COMMANDMENTS OF CYBERSECURITY

Hardware

You shall not insert unknown USBs into
the work PC

You shall not leave your PC unlocked,
even among friends or colleagues.

Software

You shall not forget backups
and will rely on redundancy.

You shall not forget antivirus software.

PeopleWare

You shall not covet another's phishing bait.

You shall take on the role of the
best line of defense against cyber-
attacks.

LocalWare

You shall not try to work
outside secure environments
and networks.

You shall not share
passwords or access
codes.

IntegraWare

You shall love cibersecurity measures
above all else.

You shall not procrastinate updates,
even on Sundays and holidays