CYBERSECURITY MANUAL

for Pharmacists

REPÚBLICA PORTUGUESA SAÚDE
40 ANOS SNS SERVIÇO NACIONAL DE SAÚDE 1979-2019
SPMS Serviços Partilhados do Ministério da Saúde
CIBERSEGURANÇA SNS

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?

- Printing patient records in pharmacies;
- Unlocked computers in public service areas;
- Sharing the same login credentials among coworkers;
- Clicking on suspicious or unverified hyperlinks.

DON'T FORGET: PATIENT SAFETY ALSO DEPENDS ON CYBERSECURITY SAFETY!

Just as in the pharmacist's daily routine, whether working in a community or hospital pharmacy, the effective treatment of patients depends on the correct administration of therapy, it is also part of the pharmacist's role to protect patients from the exposure of their personal data to third parties, as well as from unauthorized access, alteration, destruction, or loss of access.

HOW TO ACT?

JUST LIKE...

We check medication stock daily, process incoming orders, and remove batches for quality-related reasons.

WE MUST ALSO...

Confirm that there are no pending system updates to install or unresolved error messages to address.

JUST LIKE...

We write off medications by scanning their barcodes

WE MUST ALSO...

Always log out of your session after using the system for a certain period.

JUST LIKE...

There is a standard for identifying medications (e.g., the name of the active substance, dosage, batch number, and expiration date).

WE MUST ALSO...

Follow best practices for creating passwords, such as using a long passwords that include numbers, uppercase and lowercase letters and special characters.

JUST LIKE...

We advise our patients to follow the prescribed antibiotic dosage to prevent the development of resistance

WE MUST ALSO...

Be aware that new malware emerges every day, which is why we must keep our systems up to date.

JUST LIKE...

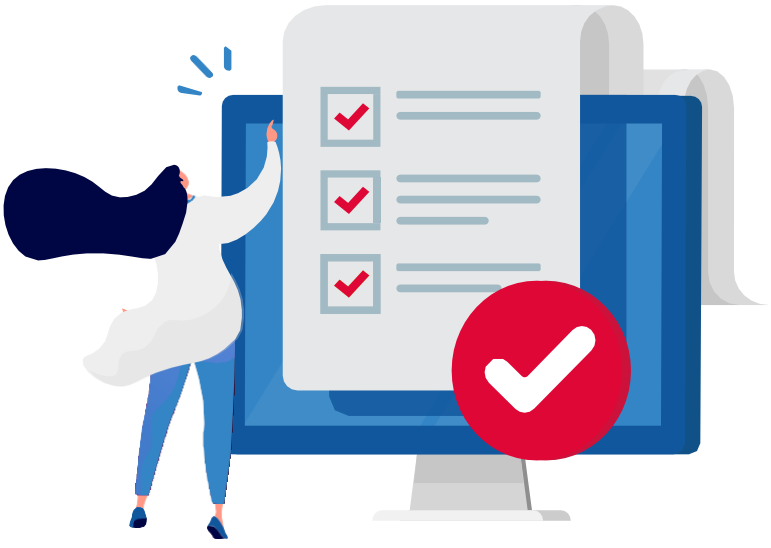
We do not share lab coats with our colleagues, nor do we share the strips and needles used for measuring biochemical parameters

WE MUST ALSO...

Use only your own access credentials in systems and never those of your colleagues.

JUST LIKE...

Before dispensing any medication to a patient, we confirm whether there are any contraindications that advise against its use



WE MUST ALSO...

We check the list of authorized software before installing anything on the professional computer, as installing unauthorized programs may lead to malware that could compromise the data stored on that PC and even affect other systems.

JUST LIKE...

We protect our patients' health by providing guidance on how their medication should be taken

WE MUST ALSO...

Protect systems by not opening or clicking on hyperlinks from unknown sources.

JUST LIKE...

We listen carefully to the patient's symptoms and provide individual, personalized counseling

WE MUST ALSO...

Follow the best practice of using a different password for each system and device, minimizing the risk of password theft and its potential consequences.

JUST LIKE...

We review the patient's medical history and contact the physician if there is a potentially harmful drug interaction

WE MUST ALSO...

Contact the IT Department/Technical Support if we have any questions related to information security and cybersecurity, or if we need to report an incident.

JUST LIKE...

In hospitals, we handle and prepare certain medications individually based on each patient's specific needs, always within the Laminar Flow Cabinet, for reasons of sterility and safety

WE MUST ALSO...

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

JUST LIKE...

We undergo training to administer injectables to patients and stay up to date on new therapeutic options

WE MUST ALSO...

Carry out awareness-raising activities on Information Security and Cybersecurity and also be familiar with the procedure to follow in the event of an incident.

JUST LIKE...

Before measuring a patient's blood pressure, we engage in a brief conversation to help them relax and avoid influencing the results

WE MUST ALSO...

Read each email carefully and always be suspicious if it has malicious origins or intentions.

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