enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

CYBER HYGIENE IN THE HEALTH SECTOR

CYBER HYGIENE PRACTICES

Health entities across Europe are increasingly reliant on digital solutions - from electronic health records and telemedicine to connected medical devices and AI-powered diagnostics. This digital transformation also brings greater exposure to cyber threats such as ransomware, phishing and the exploitation of system vulnerabilities, which can disrupt critical services, compromise patient safety, and undermine trust.

Fortunately, many of these risks can be mitigated through relatively straightforward measures, including regular system updates, secure backup management, and multi-factor authentication, which can prevent the vast majority of common cyberattacks.

This booklet, developed by ENISA, provides clear and targeted guidance with practical steps that health entities can take to:

- Safeguard sensitive data
- Minimise exposure to common cyber threats
- Strengthen overall cyber resilience.

This guidance is intended for both large hospitals and healthcare providers, as well as smaller entities, such as specialist clinics and General Practitioners, which often lack the resources but remain equally vulnerable to cyber-attacks.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PROTECT YOUR SYSTEMS & MEDICAL SERVICES

KNOW YOUR ICT ASSETS

- Manage system and software settings.
- Scan and monitor all connected systems and devices.
- Label and ringfence legacy systems.

SECURE SYSTEM CONFIGURATIONS

- Change default passwords.
- Disable unnecessary ports and services.
- Uninstall unnecessary software.

ACCESS CONTROL

- Manage and monitor administrative privileges.
- Apply the least privilege principle.
- Enforce strong passwords and consider providing a password manager to employees.
- Require multi-factor authentication (MFA) especially for online accessible systems.

PROTECT YOUR SYSTEMS & MEDICAL SERVICES

STAY UP-TO-DATE

- Install the latest security patches on all devices.
- If it can't be patched, ringfence it.
- Enable automatic periodic updates on any system that is not critical or vendor-restricted.
- Scan all systems and devices for unpatched vulnerabilities and outdated software.

MALWARE PROTECTION AND SECURITY LOGGING

- Deploy malware protection solutions.
- Allow only authorised apps and software.
- Review logs for failed login attempts, privilege escalations, and malware alerts.

BACKUPS OF CONFIGURATIONS, SOFTWARE AND DATA

- At least one backup copy must be ransomware resilient or offline.
- Perform integrity checks.
- Test backup restoration.
- Be aware of data retention periods.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PROTECT YOUR NETWORKS

HARDEN YOUR NETWORKS

- Use secure network protocols.
- Apply network segmentation.
- Have 24/7 flow monitorig & alerting.

CORPORATE EMAIL PROTECTION

- Enable hosted spam / phish filtering.
- Turn on attachment & link scanning (sandbox / safe links).
- Enforce secure protocols to block domain spoofing.

SECURE WI-FI

- Use latest wireless encryption standards.
- Isolate guest Wi-Fi from clinical LAN.
- Hide SSIDs for sensitive internal networks.
- Create strong Wi-Fi passwords.

FORTIFY INTERNET ACCESS

- Deploy next-gen firewalls.
- Apply web application filters.
- Shield your internet facing systems with Web-Application Firewall (WAF) and DDoS mitigation service.
- Enforce the use of VPN and MFA when off-site.

MIND THE SECURITY OF SMARTPHONES & E-CARE

MIND THE SECURITY OF PATIENT OPERATED DEVICES

- Design controls to ensure that no lasting harm occurs when the device is lost, stolen, or misused.
- Use strong individual credentials.
- Enforce auto-logout and wipe browser/app data in case of inactivity.
- Provide clear security recommendations.

ENABLE SECURE MOBILE USE

- Allow the installation of approved apps only.
- Enable remote-wipe if device is lost.
- Enforce strong passwords and encryption of sensitive data.
- Apply a 30-second automatic device lockout.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

KEEP PATIENT RECORDS SAFE

CLASSIFY & SAFEGUARD

- Identify sensitive data.
- Tag data based on sensitivity levels.
- Encrypt data at rest and in transit.
- Implement metadata cleaning processes.

LOG AND MONITOR

- Log and monitor all access to health records.
- Check systems for unauthorised access or data leaks.
- Alert on unusual activity.

PROTECT DEVICES & DATA

- Never leave devices unattended.
- Enforce a clean-desk/ clear-screen policy.
- Secure printing of data.
- Secure asset lifecycle (disposal or reuse).
- Verify vendor SLAs for cloud EHR & hosted apps.
- Ensure patient data access in an emergency.

TAKE INCIDENTS SERIOUSLY

BE PREPARED

- Establish an incident response process.
- Create a team and assign roles and responsibilities.
- Know and communicate who to contact in case of a cyber incident.
- Plan for the worst-case scenario.
- Perform vulnerability scans and penetration tests.

OPERATIONAL COLLABORATION

- Establish collaboration with suppliers, Managed Security Service Provider, other hospitals and peers.
- Contact your national CSIRT or supervising authority in case of a relevant incident and follow their instructions.

DISASTER RECOVERY

- Unplug equipment safely if there's smoke, water, or power issues.
- Use critical devices with an uninterruptible power source.
- Test UPS/generator fail-over.
- Include floods, fires or power outages in your Data Center Recovery Plan.

MANAGE THE ICT SUPPLY CHAIN

PROCURE SECURELY

- Involve IT department.
- Include security requirements at the earliest stage.
- Verify supplier compliance with standards.
- Ensure the security of onboarding and offboarding procedures of suppliers through the SLA agreement.

SUPPLIER RELATIONSHIP

- Restrict access to minimum necessary and secure dedicated remote connections.
- Define incident reporting and establish procedures for incident response.
- Know who to contact for security issues relating to suppliers.

CYBER EDUCATE YOUR STAFF

STRATEGY

- Train by role.
- Adapt content to audience.
- Use peer-to-peer learning.
- Train the trainers.
- Make it practical.
- Document training courses.

AWARENESS ACTIVITIES

- Phishing simulations.
- Intranet pages, staff newsletters.
- Learning sessions.
- Awards.
- Escape room.

TRAINING ACTIVITIES

- Ransomware simulation.
- Gamified quiz about cybersecurity.
- Cybersecurity exercises.
- Case studies.

PHYSICAL SECURITY

PERIMETER

- Make sure staff and contractors always wear a badge.
- Maintain intrusion alarms.
- Log every entry and exit.
- Encourage approaching persons that do not seem authorised to physically access an area.
- Audit camera coverage and store 30 days of footage.

SECURE WORKSPACES & FACILITIES

- Physically secure devices, cables & USB sticks.
- Use fire suppression.
- Check heating, ventilation and air conditioning (HVAC).
- Know where the emergency exits and fire alarms are.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: **www.enisa.europa.eu**.

Catalogue number: TP-01-25-024-EN-N
ISBN: 978-92-9204-720-7
DOI: 10.2824/3818935

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union