ACRO

Cybersecurity Essentials:
A Practical Guide

Introduction

This best practice guide has been developed by the ACRO CISO Committee to support hospitals, and other health care facilities, particularly those with limited budgets and minimal dedicated cybersecurity staff, in strengthening their cyber defenses. The cyber threat landscape has grown significantly more complex and aggressive over the past number of years, with hospitals increasingly targeted by ransomware, phishing, and other malicious attacks that directly impact patient care and essential services. Recognizing the urgent need for practical, cost-effective solutions, this guide offers actionable recommendations and highlights free and discounted resources available from industry leaders such as Microsoft and Google.

Our goal is to promote more resilient and secure healthcare environments, regardless of size or funding. This document is designed to reflect core cybersecurity best practices and is not intended to be exhaustive, but rather to provide a foundational baseline for secure operations.

> Drafted by cybersecurity professionals, this guide does not provide legal advice; for any questions relating to compliance with local, national, or other laws or regulations, consult an attorney with knowledge of cybersecurity requirements and obligations.

Essential Cybersecurity Practices on a Tight Budget

1. Risk & Asset Assessment

- Perform a basic IT audit to inventory systems (servers, workstations, EHRs).
- Identify critical data repositories (such as those containing PII or PHI), the IT systems that host them, and the security controls applied to protect the data
- Identify highest-risk areas: web access, email systems, guest Wi Fi

2. Maintain up-to-date Patching

- Enable automatic OS and third party software updates.
- Even basic patching prevents many attacks
- Prioritize patching technologies that are visible from the internet

3. Use Endpoint Protection

- Deploy EDR (Endpoint Detection & Response) Technology
- Deploy affordable antivirus/endpoint tools (Microsoft Defender AV)
- Ensure automatic updates

4. Email Scanning & Protection

- Scan all inbound and outbound emails for malware, phishing
- Implement SPF, DKIM, and DMARC to prevent spoofing and ensure domain authenticity
- Flag external emails with clear warnings to help users recognize potential phishing
- Enable TLS encryption for email in transit to secure communication

5. Implement Strong Password Policies and MFA

- Enforce complex passwords and timezone-based expiries.
- Enable multi factor authentication, especially for email, VPN, admin accounts
- Avoid SMS for MFA authentication; instead use an authenticator app or a hard token

6. Encrypt Sensitive Data

- Enable full disk encryption on laptops/tablets such as BitLocker
- Encrypt backups and transmissions
- Maintain up to date TLS

7. Train Staff on Phishing & Awareness

- Run periodic phishing drills, poster reminders, and share incident stories
- Awareness is key, human error is behind ~41% of breaches

8. Backup and Recovery Plans

- Treat backups as policy, not optional.
- Use regular, encrypted backups (cloud or onsite), test restores often
- Store backups off-site regularly
- Secure access to backups with MFA and enable immutable backups where possible

9. Network Segmentation & Guest Wi Fi

- Separate clinical systems from guest networks. Ideally, remove guest Wi Fi entirely

10. Restrict Admin/Privileged Access

- Create separate admin and user accounts
- Disallow local admin for employees
- Remove unused accounts promptly

11. Regular Vulnerability Scans & Risk Assessments

- Run basic vulnerability scans with free tools (e.g., from CISA).
- Schedule at least quarterly focused reviews

Low-Cost Tools & Cloud Options

Antivirus:
Microsoft Defender AV

Full-Disk Encryption:
Built-in OS tools (e.g., Windows BitLocker)

Free/Phased Periodic Backups:
Use encrypted cloud storage plans

Free/Low-Cost Scanning & Phishing Tests:
From CISA

Cloud-Based Email Filtering and MFA:
Utilize Microsoft 365 or Google Workspace's security features

Free & Discounted Programs for Rural Hospitals (U.S.-focused)

Microsoft Cybersecurity Program for Rural Hospitals

- Available to U.S. rural hospitals, including **Critical Access** and **Rural Emergency Hospitals** Sign up for the Cybersecurity Program for Rural Hospitals
- **Includes:**
  - Free security assessments by Microsoft-trusted partners;
  - Cyber-awareness training for frontline & IT staff;
  - One year of Microsoft 365 E5 Security suite (or 75% off nonprofit pricing for smaller orgs);
  - Extended Windows 10 security updates;
  - AI innovation support (e.g., Rural Health AI Lab)
- **Impact:** Over **550 rural hospitals** registered; ~375 assessments done; ~1,000 staff trained How Microsoft is helping rural communities protect critical healthcare infrastructure.

European Union Agency for Cybersecurity

ENISA offers **free support** to help hospitals and healthcare providers across the EU improve their cybersecurity resilience. This is part of a broader EU initiative launched in January 2025 to address the growing threat of ransomware, data breaches, and other cyberattacks targeting the health sector. Once established this center will offer:

- **Tailored guidance and best practices** for cybersecurity and procurement.
- **Regulatory mapping tools** to help hospitals comply with NIS2 and other EU regulations.
- **Early warning services** to detect and alert on emerging threats.
- **Incident response playbooks** for ransomware and other common attack scenarios.
- **Training and capacity-building** through the EU Cyber Skills Academy and Cybersecurity Skills Framework

While the Support Centre is still being operationalised, hospitals can **start engaging now**:

- **Join the EU Health ISAC** by emailing eh-isac@z-cert.nl
- Membership is free and voluntary

Google’s Rural Healthcare Cybersecurity Initiative

- Targeted at rural U.S. healthcare systems
- **Offers:**
  - Free endpoint security advice;
  - Discounted migration via Workspace (HIPAA eligible) and Chrome Enterprise;
  - Free Mandiant cybersecurity courses through Health-ISAC;
  - Funding support for software migration;
  - Pilots for custom security packages;
  - Support for cybersecurity clinics in universities serving local hospitals

How to Access

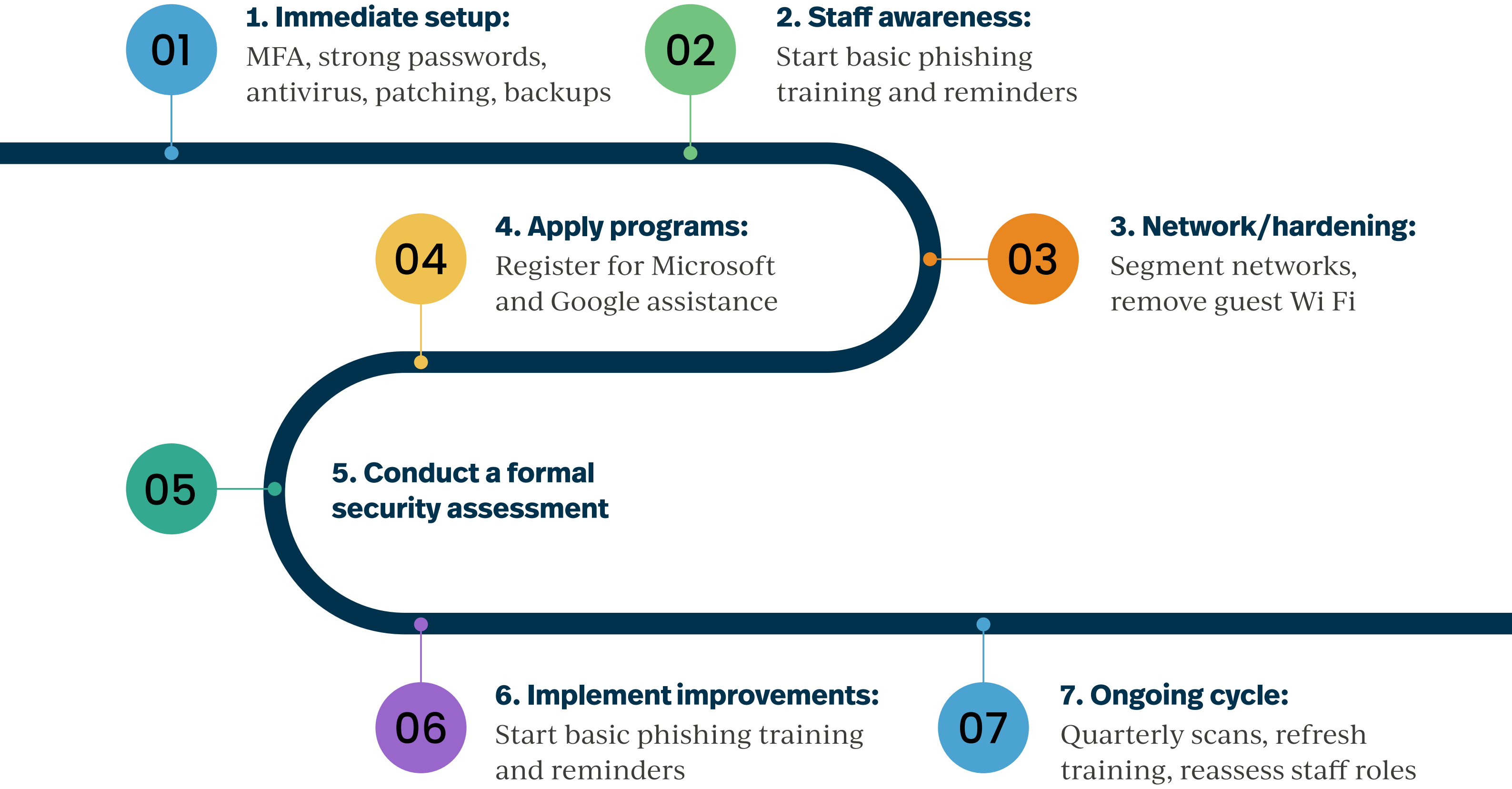
1. Check rural eligibility definitions (HRSA criteria)
   Health Resources & Services Administration Criteria

2. Sign up via Microsoft’s program portal
   Sign up for the Cybersecurity Program for Rural Hospitals

3. For Google, reach out through Google Cloud’s rural healthcare initiative page
   Google’s rural healthcare cybersecurity initiative

4. Engage with Health-ISAC groups for access to free training modules and threat intel

Priority Roadmap for a Lean IT Team



1. Immediate setup: MFA, strong passwords, antivirus, patching, backups

2. Staff awareness: Start basic phishing training and reminders

3. Network/hardening: Segment networks, remove guest Wi Fi

4. Apply programs: Register for Microsoft and Google assistance

5. Conduct a formal security assessment

6. Implement improvements: Start basic phishing training and reminders

7. Ongoing cycle: Quarterly scans, refresh training, reassess staff roles

Summary

Even hospitals and other health facilities with very limited budgets can significantly reduce cyber risk through basic hygiene: patching, scanning, access control, backups, and awareness. And for U.S. rural hospitals, both Microsoft and Google now offer free or discounted cybersecurity services and resources from assessments and training to tooling and migration support. These programs are already helping hundreds of hospitals strengthen their defenses and resilience.

ACRO

Innovate
Advocate
Collaborate