Cyber Hygiene in Scrubs:

Simple Security Habits Every Healthcare Worker Should Know

Office of Information Technology
Division of Information Security
SEPTEMBER 2025

At IHS, hygiene saves lives. But while we are washing hands and wiping down surfaces, another invisible threat lurks just beyond the exam room: cyber threats. From phishing emails to hijacked medical devices, the digital world needs as much care as the physical world.

Welcome to the world of **cyber hygiene** – your new best friend in protecting patients, privacy, and your hospital's reputation. And do not worry: No IT degree is required!

What Is Cyber Hygiene, Anyway?

Think of cyber hygiene as the digital version of hand washing. It is the practice of keeping your devices, data, and online behaviors clean and secure to prevent infections (**malware**), breaches (**data leaks**), and misdiagnoses (resulting from **clicking suspicious links**).

Just like handwashing has become second nature, good cyber habits can, too!

Don't Let Your Passwords Go Unwashed

The Problem: "Password123" is the digital equivalent of not scrubbing before surgery.

The Fix:

- Use long, complex passwords (passphrases are even better—think "HeartMonitor$HumidTulip97")
- Don't reuse passwords across different accounts!
- Consider a password manager – it's like a pillbox for your logins!

Be Suspicious of Strange Symptoms (aka Emails)

The Problem: Phishing emails look more convincing than ever. One click, and ransomware spreads faster than the flu.

The Fix:

- Hover over links before clicking
- Check for spelling errors or odd sender addresses
- If it feels weird, report it to IT – better safe than sorry

Lock It Down, Even in the Break Room

The Problem: Shared workstations and devices can leak more data than an IV bag with a hole.

The Fix:

- Always log out when stepping away, even for what you think is a quick break
- Use badge-activated systems if available
- Keep physical files secure, too – cyber hygiene includes real-world habits

Update = Immunize Your Devices

The Problem: Ignoring software updates is like missing a scheduled vaccine.

The Fix:

- Enable automatic updates for apps and systems
- Restart devices regularly to complete updates
- Notify IT if something seems off or out-of-date

Don't Share Devices Like You Share Stethoscopes

The Problem: Believe it or not, IHS devices can carry digital infections.

The Fix:

- Use IHS-approved devices when accessing patient info
- Avoid plugging unknown USBs into any system (yes, even if it's labeled "lab results")
- Do not download apps without IHS IT approval

Cybersecurity is a Team Sport

You don't have to be in IT to be part of the cyber defense team. Many breaches start with human errors, which can be fixed with awareness, teamwork, and a few smart habits.

So next time, just as you sanitize your hands, take a second to sanitize your digital behavior too!

Because at IHS, prevention is always better than a cure, especially when it comes to cyber threats.

Stay vigilant and always report any incidents or suspicious activities via email to your Area ISSO or the IHS Cybersecurity Operations Team at incident@ihs.gov.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.