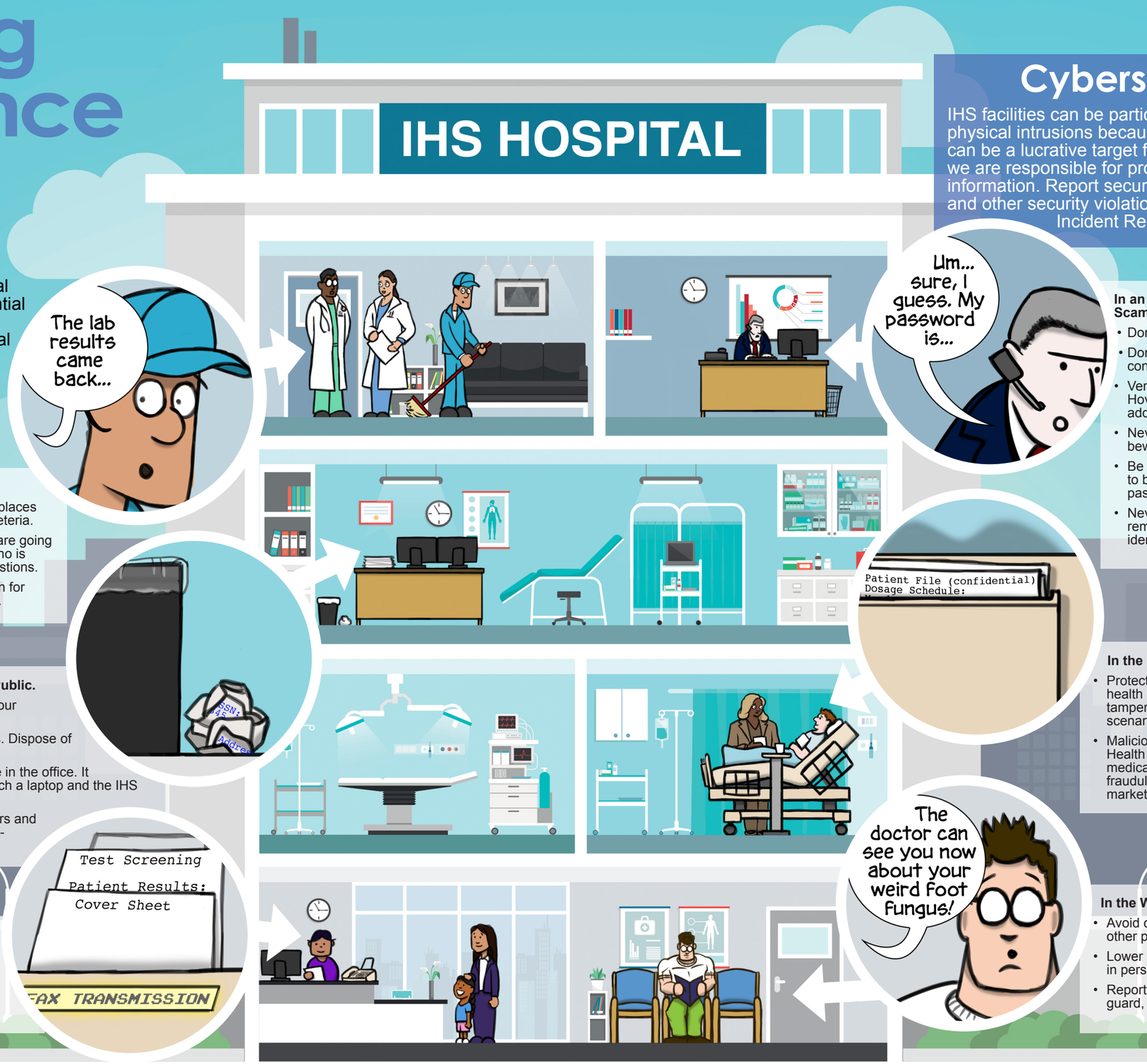
Building Resilience @ IHS

National Cybersecurity Awareness Month

The link between cyber and physical security is essential to the resiliency of critical infrastructure. Resilience of essential systems and assets, from power grids to healthcare systems, is vital to our national security, economy, and public health and safety. This week's bulletin looks at the cyber and physical security of IHS healthcare facilities.

Cybersecurity Tip

IHS facilities can be particularly vulnerable to cyber and physical intrusions because we have patient data, which can be a lucrative target for criminals. As IHS employees, we are responsible for protecting patient and personal information. Report security incidents, phishing attempts, and other security violations to the IHS Cybersecurity Incident Response Team at csirt@ihs.gov.



In Common Areas, Use Common Sense.

- Be discrete discussing patients in public places like elevators, public hallways, or the cafeteria.
- Ask unaccompanied visitors where they are going and if they have a visitor ID. Someone who is supposed to be there won't mind the questions.
- Never hold a door to a secured area open for anyone who doesn't have appropriate ID.

In a Vacant Office, Consider the Space Public.

- Always remove your PIV card and lock your computer when you walk away.
- Don't leave sensitive papers in trashcans. Dispose of them properly (like by shredding them).
- Secure your portable devices, even while in the office. It takes only a second for someone to snatch a laptop and the IHS data on it.
- Remember that other people (like cleaners and maintenance workers) access open work-spaces outside normal hours.

In Patient Registration, Be Aware.

- Position your computer screen so that others can't see it.
- Remove documents promptly from fax and copy machines.

In an Occupied Office, Be Vigilant Against Scams.

- Don't open or respond to suspicious emails.
- Don't open attachments or downloads without confirming they're legitimate.
- Verify a link is legitimate before clicking on it. Hover over it with the mouse to reveal the web address.
- Never forward spam or chain letters, and beware of phishing attempts.
- Be cautious of telephone scammers claiming to be tech support. Don't give them your password or install their software.
- Never trust unsolicited phone calls or give remote access to any individual unless the identity of that person can be verified.

In the Patient's Room, Protect Patient Data.

- Protecting patient data is critical because hacking health records could lead to altered drug dosages, tampered treatments, or other devastating scenarios.
- Malicious actors could also use Protected Health Information to gain access to medical care or prescription drugs for fraudulent use or to resell on the black market.

In the Waiting Room, Be Discrete.

- Avoid conversations about one patient in front of other patients or their visitors.
- Lower voices when discussing patient information in person or over the phone.
- Report suspicious people or activity to the security guard, supervisor, or management official.