By Alex Walker and Gabriel Sindelar

Cybersecurity in Healthcare

Why We Chose This Topic

It affects real people, not just systems.

It shows the human side of cybersecurity.

It’s relevant to our careers.

Healthcare is one of the most targeted industries.

Recent attacks show the stakes.

What Attacks?

Change Healthcare Attack (2024)

Largest healthcare data breach in U.S. history — impacted 192+ million people

Nationwide outages: claims, prescriptions, and eligibility systems went down

Hospitals couldn’t process payments, leading to major financial strain

Pharmacies experienced delays filling medications

Providers had to switch to manual processes, slowing down care

Even after a $22 million ransom payment, stolen data was not fully deleted

Attack caused industry-wide disruption, affecting nearly every major hospital system

Ascension Health Attack (2024–2025)

Third largest healthcare data breach in 2024 with around 13.4 million records

Canceled surgeries and appointments due to system outages

Medical devices went offline, forcing staff to use manual processes

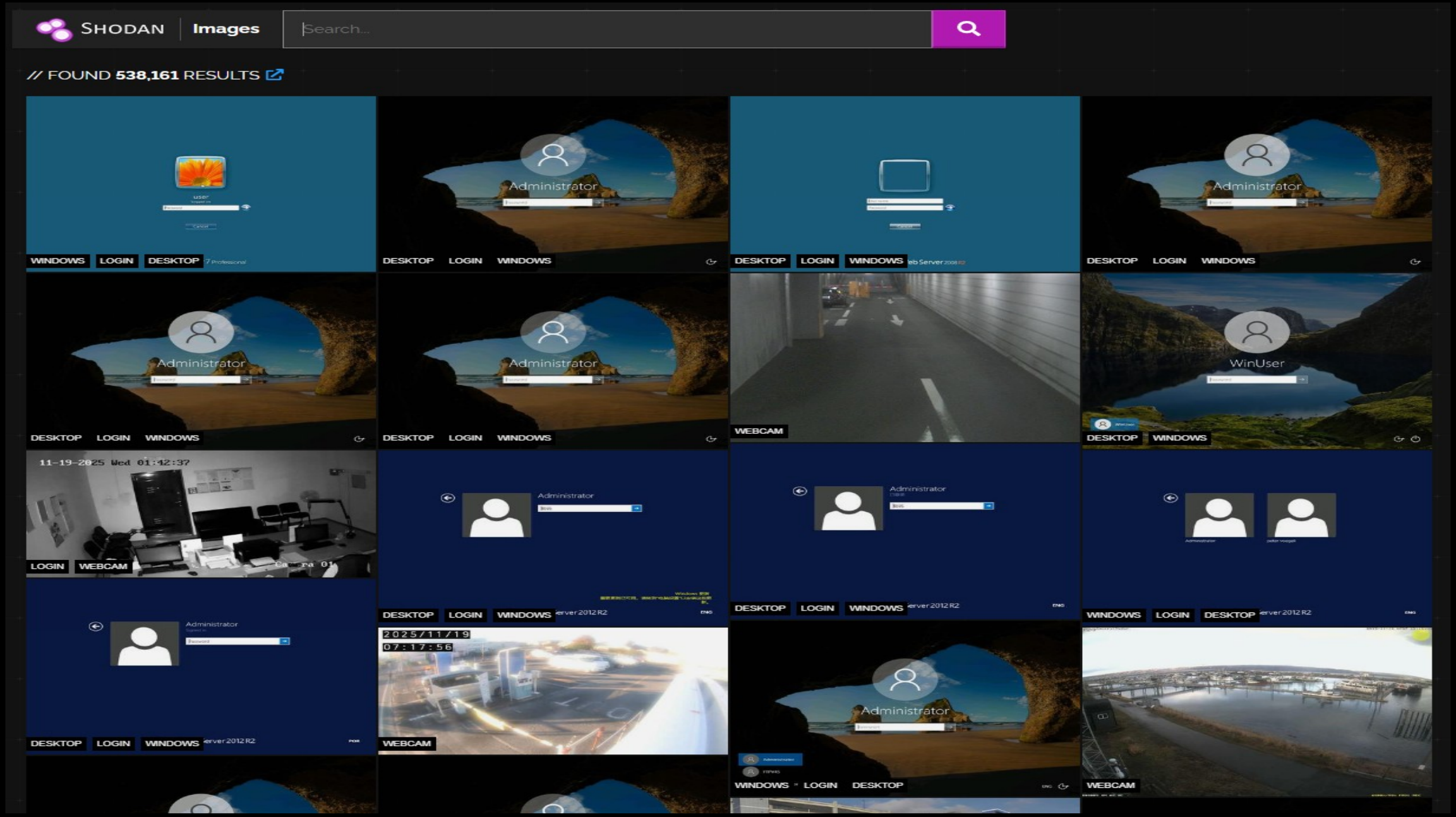
Pharmacy and prescription disruptions

Hospitals had to divert patients to other facilities

Millions in financial loss and recovery costs

Problems in Hospital Tech

- Outdated operating systems (Windows 7, XP, unsupported software)
- Unpatched vulnerabilities due to slow update cycles
- Medical devices locked to old software versions that can’t be easily upgraded
- Weak or outdated authentication systems on workstations and devices
- Legacy applications that break when hospitals try to modernize
- Lack of encryption on older machines and devices
- Old hardware that can’t support modern security requirements
- Insecure IoT medical equipment (monitors, pumps, imaging machines)


SHODAN
Images
Search...
// FOUND 538,161 RESULTS
WINDOWS LOGIN DESKTOP
DESKTOP LOGIN WINDOWS
Administrator
WEBCAM
WinUser
11-19-2025 Wed 01:42:37
LOGIN WEBCAM
2025/11/19
07:17:56

Webcams & Security Cameras	Old Windows Workstations	Medical Imaging Systems	Building & Facility IoT	Laboratory Equipment	EXTRA	EXTRA
Nurse station cameras	Windows XP, 7, Server 2003	PACS servers (hold X-rays, MRIs, CT scans)	HVAC systems	Blood analyzers	Pyxis and Omnicell systems	Known vulnerabilities
Parking/ entrance security feeds	Used for nurses' stations, radiology, lab computers	DICOM devices	Badge readers	Lab management systems	Exposed SIP servers	Patient room cameras
Often no password or default credentials	RDP open → huge ransomware entry point	Sometimes show patient names or scan previews	Environmental monitors (temperature, humidity	Often running outdated embedded OS	Attackers can listen, redirect, or flood calls	Older models broadcast open ports

Poor Infrastructure

- Outdated network architecture

Old systems are hard to secure or upgrade.

- Flat networks with poor segmentation

One breach spreads across the whole hospital.

- Too many devices on one network

Medical equipment, IoT, and workstations all mixed together.

- Limited monitoring + slow patching

Hard to detect intrusions or update critical systems.

- Tight budgets + high upgrade costs

Hospitals delay replacing hardware and network equipment.

- Cost of downtime

Upgrading systems risks interrupting patient care, so changes get postponed.

Human Behavior + Insider Risks

What People Do

- Fall for phishing emails and fake update pop-ups
- Click links because they’re stressed, tired, or rushed
- Peek at patient records out of curiosity (huge violation)
- Use weak or shared passwords across departments

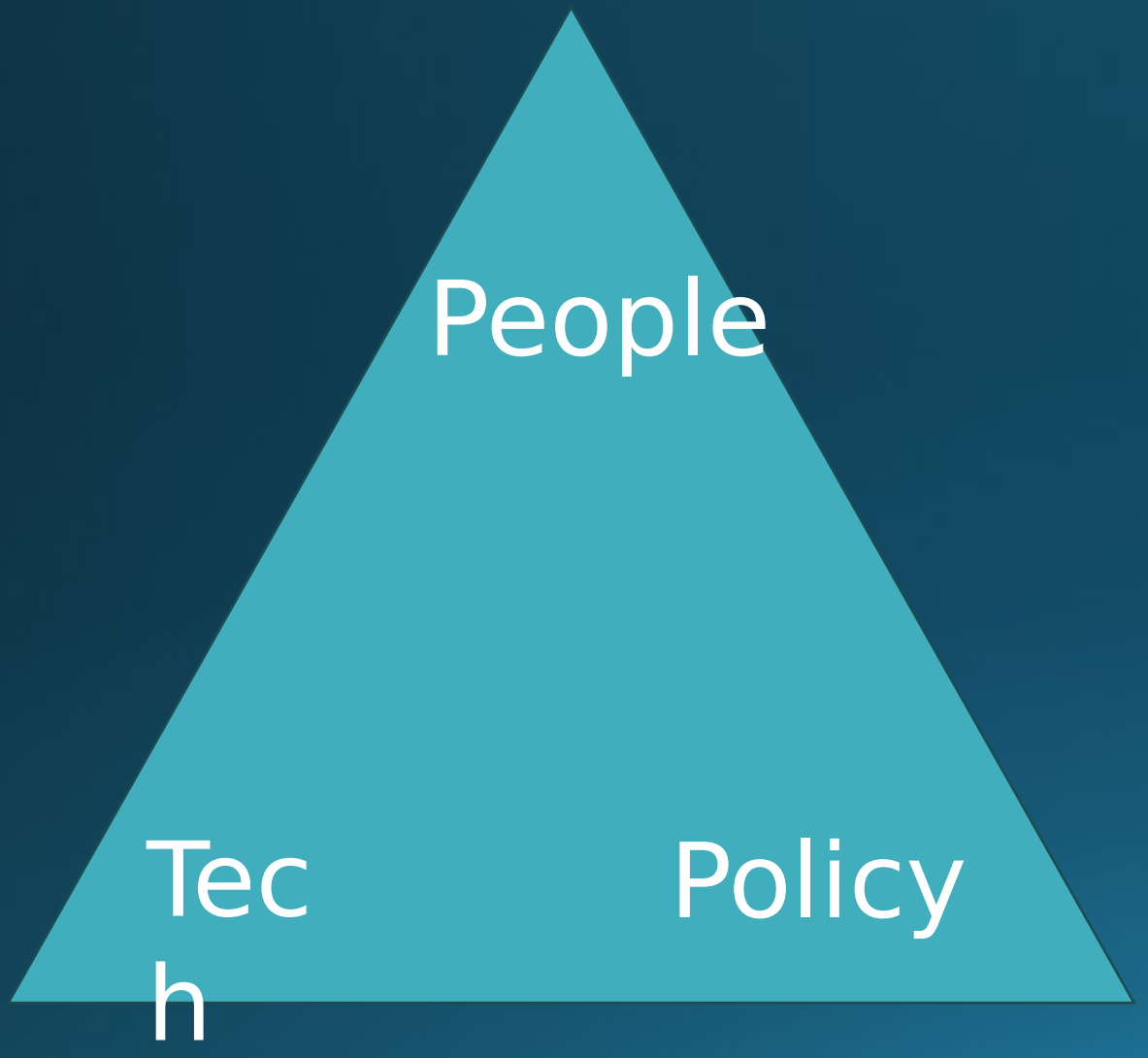
Why It Happens

- High-pressure environment affects judgment
- Human psychology: habits, stress, urgency
- Low priority on cyber training until something breaks
- Work culture: “just get through the shift”

Governance and Compliance

Federal Laws	State Laws	Hospital Policy
HIPAA	Virginia Data Breach Laws	Password Policy
HITECH	Medicaid Out Of State Laws	Patient Privacy Policy
		Hardware Configuration Management Plan

Prevention



PEOPLE

Human behavior is the biggest factor in healthcare security. Staff under stress click phishing links, reuse passwords, or bypass rules to save time. Training and awareness directly shape how safe a hospital actually is.

TECH

Security tools like encryption, MFA, secure networks, updated devices, and monitoring systems help defend hospitals. Good tech reduces risk, but it only works if people use it correctly.

POLICY

Policies like HIPAA, HITECH, and Zero Trust set the rules: who can access data, how it must be protected, and what happens in a breach. Strong policies guide both people and technology toward safer practices.

Conclusion

Segment legacy devices from the network

Policy should work with the routine of the people

PII and PHI make hospitals a target for threat actors

Compliance with state and federal laws keep hospitals safe

References

Alder, S. (2020, March 12). *83% of medical devices run on outdated operating systems*. The HIPAA Journal. https://www.hipaajournal.com/83-of-medical-devices-run-on-outdated-operating-systems/

Alder, S. (2025, April 3). *What is the Hitech Act? 2025 update*. The HIPAA Journal. https://www.hipaajournal.com/what-is-the-hitech-act/

Center for Disease Control. (2024, September 10). *Health Insurance Portability and accountability act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

D. Locking, interview in Monarch Hall, October 22nd, 2025

Harpur, R. (2025, July 24). *Ascension ransomware attack: Impact and prevention tips*. BlackFog. https://www.blackfog.com/ascension-ransomware-attack/

House Committee on Energy and Commerce. (2024, May 3). *What we learned: Change healthcare cyber attack*. https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022, December 2). *Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021*. JAMA health forum. https://pmc.ncbi.nlm.nih.gov/articles/PMC9856685/

Shodan: https://www.shodan.io/