

# Cybersecurity in Healthcare:

Trinity Howard, Alice Vanty, and






# Agenda

- Social Science: The Psychology of Risk
- Challenges in the healthcare sector
- Protection of patient data

—

# Social Science: The Psychology of Risk





# Social Science: The Psychology of Risk

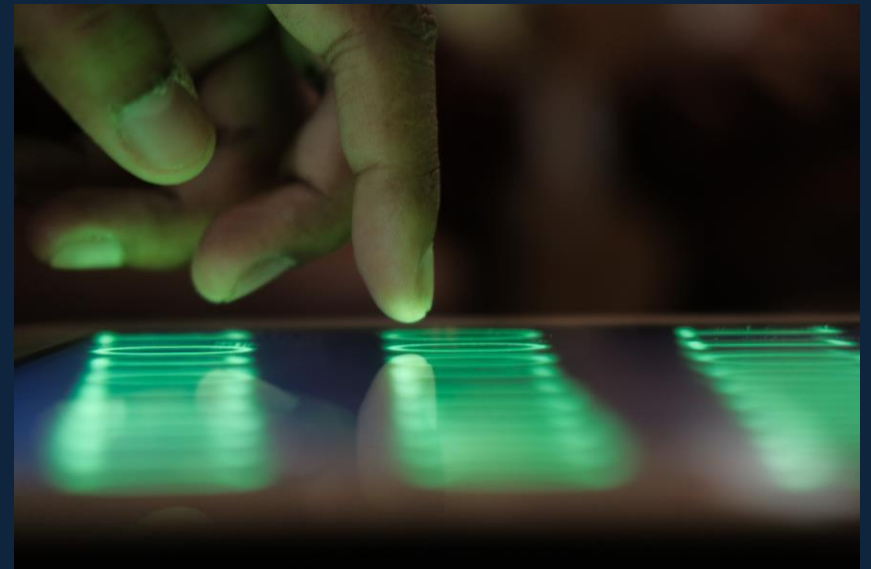
- Cybersecurity isn't just code it's psychology. Attackers exploit human emotions, urgency, fear, and helpfulness.
- **Burnout Factor:** Healthcare workers operate under high stress. Cognitive fatigue makes them significantly more susceptible to phishing emails and social engineering tactics, bypassing even the best technical firewalls.

# Why Hackers Love Hospitals

## Credit Cards vs. Medical Records:

If your credit card information is stolen fraud stops, But you cannot cancel your medical history, your genetics, or your past surgeries.

This permanence makes a medical record worth up to \$1,000 on the black market, compared to just \$5 for a credit card. It is the ultimate tool for identity theft.





# Challenges in the healthcare sector

---



# Challenges in the healthcare sector

- Legacy medical devices: running outdated software create unfixable vulnerabilities within hospital networks.
- Exhaustion: staff are highly susceptible to sophisticated phishing attacks, serving as the weakest security link.
- Most critically, these cyberattacks directly interrupt patient care, leading to dangerous treatment delays and physical harm.

# THE PEDIATRIC RISK: "THE 18-YEAR CON

## The Clean Slate:

Attackers target children specifically because they have "clean" credit histories and no one checks their reports.

A hacker can steal a child's ID at birth and use it to buy houses or cars, only to be discovered when the child applies for their first student loan 18 years later.



Protection of  
patient data



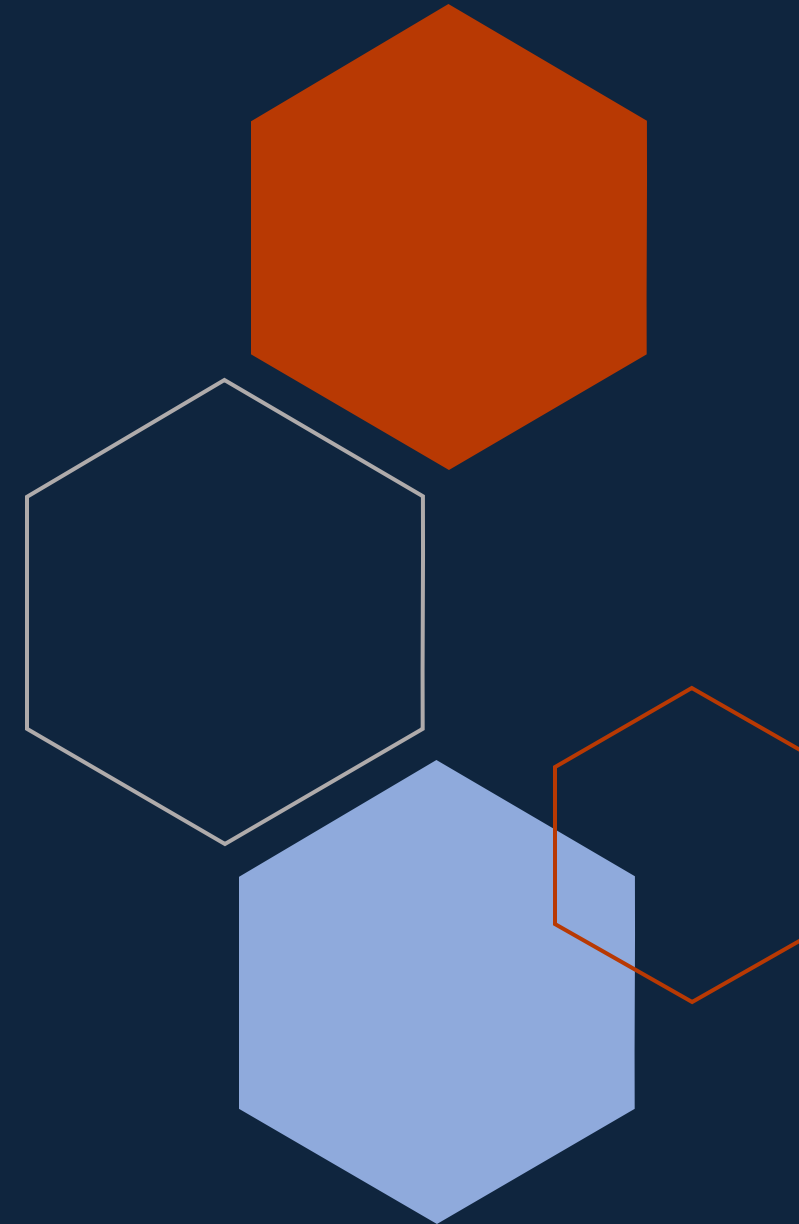
# Protection of patient data

- Security by Design: Medical devices and "smart toys" used in therapy must be built with security as a priority, not an afterthought.
- Specialized Training: Pediatric staff need training on "social engineering" that exploits their desire to help parents (e.g., phishing emails disguised as urgent parent requests).
- COPPA & Regulations: Strengthening laws like the Children's Online Privacy Protection Act to cover modern health apps and wearables.
- Credit Freezes: Educating parents to freeze their minor child's credit reports as a standard preventative measure.



# Summary:

Hospitals have a huge problem with cyberattacks. They use old medical machines and tired staff who sometimes accidentally click on bad links. This is super dangerous because hackers lock up the hospital's computers with something called ransomware. When this happens, ambulances get sent away, and people can get hurt because they can't get fast care. Hackers steal medical records because they are worth much more money than credit cards, and they sometimes even steal kids' IDs to use for years without anyone noticing. To fight back, hospitals need to use better security rules. Keeping these files safe is the number one way to keep patients safe.





**Thank you**