




Growth. Performance. Success.

NCPA 2025 ANNUAL CONVENTION

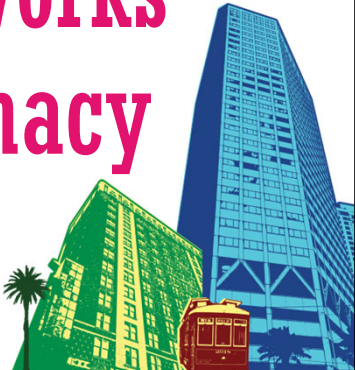


1



**Firewall Rx:
Cybersecurity Frameworks
for the Modern Pharmacy**

➤ **NCPA 2025 Annual Convention and Expo**



2

Speakers



Chris Sykes, MCSA, M.S.

Director of IT
Sykes & Company, P.A.



Scotty Sykes, CPA, CFP®

Vice President
Sykes & Company, P.A.



3

Disclosure Statement

There are no relevant financial relationships with ACPE defined commercial interests for anyone who was in control of the content of the activity.



4

Pharmacist and Technician Learning Objectives

1. Identify key cyber threats facing pharmacies.
2. Review modern best practices for preventing cybersecurity incidents.
3. Outline a pharmacy-specific incident response plan using National Institute of Standards and Technology-aligned principles.
4. List 10 critical response steps to take in the event of a suspected or confirmed security breach.



5

Pharmacy Cybersecurity Threats: Real-World Scenarios



7

Independent Pharmacy

- “Client” reaches out to accounts payable via email looking to pay a “vendor”
- “Admin personnel” replies stating that they can make the payment but may be later until they can get to it
- “Client” approves and says thanks and copies outsourced accountant
- After approval from “client” & “admin”, third-party accountant **notices a discrepancy** in the account numbers and also notices unusual amount

Independent Pharmacy

- Third-party accountant verifies via phone or text as follow up email doesn't **feel** right
- Phone call with client confirms that their email was hacked and accounts payable request was incorrect
- Payment is not processed!

Top Threats Facing Independent Pharmacies

- Ransomware
- Malware
- Phishing
- Stolen or compromised credentials
- Social engineering
- Threats often overlap:
 - Example: Most ransomware incidents begin as phishing



10

Top Vulnerabilities in a Pharmacy

- Business email compromise
- Social engineering
- Malware-infected USB devices
- Unsecured network ports and wi-fi networks
- Outdated software



11

Knowledge Check

What was this owner the victim of?

- A. Stolen or compromised credentials
- B. Phishing
- C. Social engineering
- D. All of the above



12

Incident Overview

- Hacker utilized a **phishing attack** to gain email access
- Credentials were now **compromised**
- Hacker then utilized **social engineering** to try to funnel a large sum of money to their bank account in the form of an AP request



15



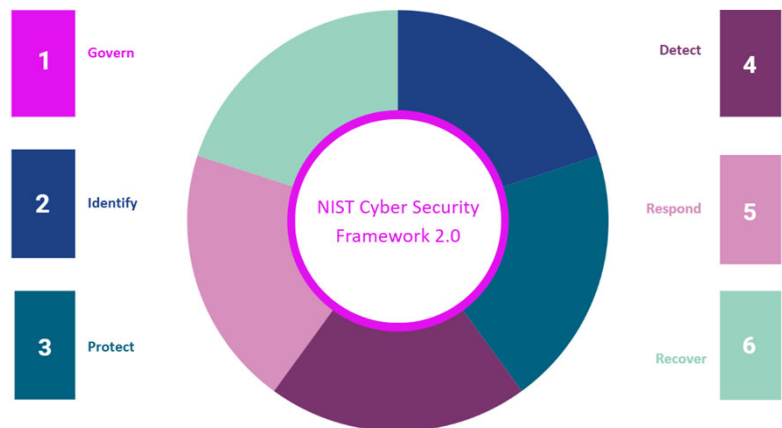
Preventing Cyber Attacks: Frameworks and Best Practices



16

NIST Cybersecurity Framework

- Developed by National Institute of Standards and Technology (NIST)
- Proactive risk management
- Third-party risk awareness
- Flexible and Scalable
- HIPAA Compliant



<https://www.nist.gov/cyberframework/quick-start-guides#smallBusiness>

17

NIST Cybersecurity Framework

- **Govern:** Acceptable use policies in place for the pharmacy and for employee-owned devices accessing business resources
- **Identify:** What are the most critical business assets we need to protect
- **Protect:** Endpoint Protection, Enabling MFA, Policies and Procedures, Network Security, Human Firewall



18

NIST Cybersecurity Framework

- **Detect:** Outcomes that help you find and analyze possible cybersecurity attacks and compromises
- **Respond:** Supports your ability to act regarding a detected cybersecurity incident
- **Recover:** Restore assets and operations that were impacted by A cybersecurity



19

Core Pharmacy Security Recommendations

- Maintaining up-to-date devices and software
- Adhering to password best practices
- Implementing two-factor authentication
- Developing a robust and comprehensive backup plan
- Regular review and assessment of security risks



20

Smart Pharmacy Cybersecurity Habits

- Using modern computers with Windows 11
- Windows defender with real-time virus definition updates
- Cloud backup services like OneDrive or Google Drive
- Biometric logins with a trusted password manager
- Controlled folder access
- Secured routers and up-to-date firmware



21

Designing Your 10-Step Breach Plan

Things to consider when designing your 10-step breach plan:

- Regulatory requirements
 - Understand HIPAA, state laws, and reporting guidelines
- Risk assessment
 - Identify likely breach scenarios
- Roles and responsibilities
- Vendor coordination
- Training and awareness



22

10-Step Breach Plan Example

Dependent on script management system...

- | | |
|--|---|
| 1. Isolate affected systems | 6. Determine the scope and impact |
| 2. Activate the incident response plan | 7. Notify law enforcement and/or regulators |
| 3. Notify your IT provider/security team | 8. Notify affected parties as required |
| 4. Preserve logs and evidence | 9. Begin remediation and recovery efforts |
| 5. Begin internal communication and staff coordination | 10. Conduct a post-incident review |



23

Knowledge Check

Before responding to a cybersecurity incident, what should a pharmacy owner be mindful of?

- A) Script management system protocols
- B) What technologies or services are personnel using to accomplish their work
- C) Are there any antivirus updates and anti malware software that needs to be installed
- D) All of the above



24

AI and Cybersecurity: Threats and Best Practices



27

AI Threats For Pharmacies

- AI augmented phishing and vishing
- Prompt injection & LLM data leakage in workflows
- Data poisoning & model supply-chain compromise
- Model extraction & privacy attacks
- Shadow AI & third-party risk

AI Augmented Phishing and Vishing

Simple phone and voice security:

- Only call back numbers you can verify
- Give staff scripts and secret passphrases to use
- Don't automatically trust voices on the phone

Safer Use of AI Models

- Keep model inputs/outputs separate from other systems
- Only let them use approved tools
- Clean up prompts before they go in
- Block personal or sensitive data
- Keep detailed logs of all activity



30

AI Model Integrity

- Track where your data and models come from
- Check and certify outside models before using
- Use test datasets that flag issues
- Run “attack” tests before launching, like you would with code



31

Privacy and API Controls

- Put limits on API usage and monitor them
- Add harmless “noise” to outputs if it helps protect privacy
- Train models in ways that keep data private
- Don't mix health data (PHI) into general models unless you have a business associate agreement and strict rules in place
 - Specific health conditions
 - Medications
 - Patient messages



32

Governance and Compliance

- Publish a list of which AI tools are approved
- Block or allow domains as needed
- Favor enterprise AI tools that sign legal data-protection agreements
- Use tools that redact or block sensitive info going in or out of AI
- Map risks and protections using NIST's GenAI framework



33



Frameworks and Best Practices in Action



34

Independent Pharmacy

- “Client” reaches out to accounts payable via email looking to pay a “vendor”
- “Admin personnel” replies stating that they can make the payment but may be later until they can get to it
- “Client” approves and says thanks and copies outsourced accountant
- After approval from “client” & “admin”, third-party accountant **notices a discrepancy** in the account numbers and also notices unusual amount **(Detect)**

35

Independent Pharmacy

- Third-party accountant verifies via phone or text as follow up email doesn't **feel** right (**Response process begins**)
- Phone call with client confirms that their email was hacked and accounts payable request was incorrect
- Payment is not processed!
- (**Recover process begins**)



36

5 Quick Wins For Your Pharmacy

- Implement MFA
- Updated Windows/Mac PCs with all updates
 - Windows 10 is end-of-life in October (ESU's available)
- Maintain all application and device updates (Office, script systems, etc.)
 - Firewalls, routers, APs, etc.
- Implement and use a password manager
- Verify who has access to what
 - Comb through all software and portals. Ensure only necessary users have admin access and that terminated staff are disabled or removed



37

Knowledge Check

When the outside party notices a discrepancy in the account numbers and unusual amount, this is an example of?

- A. Detect
- B. Creating a culture of reporting and vigilance
- C. Respond
- D. All of the above

Knowledge Check

When the outside party notices a discrepancy in the account numbers and unusual amount, this is an example of?

- A. Detect
- B. Creating a culture of reporting and vigilance
- C. Respond
- D. All of the above

Contact Information

Chris B. Sykes

Director of IT, Sykes & Company, P.A.
chris@sykes-cpa.com

Scotty W. Sykes

Vice President, Sykes & Company, P.A.
scott@sykes-cpa.com

