



# CYBERSECURITY: REAL-LIFE SCENARIOS

The U.S. government's Office for Civil Rights (OCR) recommends that health plans strengthen business defenses (i.e. safeguards) against the following three threats to cybersecurity<sup>1</sup>.



## THREAT 1: PHISHING

Phishing is used to trick individuals into divulging sensitive information, such as ePHI, by impersonating a trustworthy source<sup>2</sup>.



## SOLUTION



**Train your workforce regarding security awareness in software and e-mail usage. Your HIPAA Security Officer and IT team are responsible for regular testing of software systems and evaluating their effectiveness.**

- † Train staff on what to look for in suspicious emails
- † “Test” the system with simulated phishing emails to workforce members and assess their response

<sup>1</sup> [Q1 2022 Newsletter](#)

<sup>2</sup> According to the OCR Newsletter, 42% of ransomware attacks in Q2 2021 involved phishing.



## THREAT 2: EXPLOITING KNOWN VULNERABILITIES

Hackers can penetrate networks and gain access to ePHI by exploiting known vulnerabilities.

Vulnerabilities may exist in many parts of your IT infrastructure, including:

- † server, desktop, and mobile device operating systems
- † application database, and web software
- † router, firewall, and other
- † device firmware



## SOLUTION

### Uncover and address vulnerabilities by:

- † Conducting a thorough Risk Analysis (RA)
- † Documenting and maintaining RA results

### Mitigate known vulnerabilities by:

- † Applying vendor patches or upgrading to a newer software version.
- † Upgrading or replacing obsolete, unsupported applications and devices (i.e., legacy systems).
- † Implementing a security management process to prevent, detect, contain, and correct security violations, including conducting a risk analysis!



## THREAT 3: WEAK CYBERSECURITY PRACTICES

Strong practices include complex password rules and dual factor authentication.

80% of breaches are due to hacking involving compromised credentials<sup>1</sup>.



## SOLUTION

- Verify that persons or entities seeking access to ePHI are who they claim to be by implementing authentication processes.
- Implement results from the risk analysis to better protect ePHI (e.g., which authentication solutions did you discover are best for your business?).



<sup>1</sup> [Q1 2022 Newsletter](#)



877.328.7880

[www.compliancedashboard.net](http://www.compliancedashboard.net)

*Content is not and should not be construed as legal advice and is for education purposes only. Verify with counsel both federal and state laws applicable to your Plan decisions.*