Cybersecurity for healthcare: Strategies to mitigate the risks

"On Legal Grounds" provides a general informative overview of the topics addressed. It is provided with the understanding that the author is not engaged in rendering legal advice. The guidelines suggested here are not rules, do not constitute legal advice and do not ensure a successful outcome. The ultimate decision regarding the appropriateness of any treatment must be made by each healthcare provider considering the circumstances of the individual situation and in accordance with the laws of the jurisdiction in which the care is rendered.

By Richard F. Cahill, JD

An East Coast plastic surgery group paid a $2.6 million settlement in spring 2026 after patient data was stolen during a ransomware attack. The complaint filed by its patients alleged that the group had failed to take basic cybersecurity precautions.

Malicious software can prevent an organization from accessing its data unless payments are made, which can interfere with patient treatment. Further, ransomware attacks can include data breaches – and a covered entity's inadvertent violations of federal and state privacy laws may result in civil, criminal and administrative dangers.

Through advance planning and collaboration with trusted business partners, healthcare organizations can mitigate their cybersecurity risks – including risks engendered by technological advancements, agency oversight and third-party vendor relationships.

AI risks and rewards

AI amplifies certain digital risks for plastic surgery practices, with or without the presence of cybercrime:

- AI tools can connect the dots between disparate pieces of information. Therefore, previously deidentified patient photos may not stay deidentified. Private patient photos can even come up in Google searches of patient names.

AI also adds new weapons to the cybersecurity fight. Some experts espouse an advantage to defenders, but new risks include:

- Some cybercriminals find an entity's vulnerabilities, then sell their access to other bad actors, who then carry out the actual malicious strike. The time window for handing over these access points has shrunk from hours down to seconds.
- Technological advancements are enabling malicious actors to produce increasingly convincing phishing attempts: A large proportion of serious cyber threats to healthcare come through contact with employees.

Regulatory, compliance risks

When patient records are violated, federal and state privacy laws create added risks to clinicians, practices and systems:

- Complaints from government agencies: Data breaches often lead to complaints initiated by agencies including the Office for Civil Rights, with possible investigations resulting in fines, sanctions and related administrative penalties.
- Loss of privileges: Harm to affected clinicians may include limitations to, or a complete loss of, admitting and surgical privileges at a medical facility or possibly exclusion from third-party payer networks – including CMS.

Third-party risks

Cybercriminals can aggressively strike third-party vendors that support medical and dental practitioners. When data breaches begin through a third party, they can take longer to identify, cause more disruption and cost more to contain than a direct attack.

Strategies to mitigate risks

Healthcare organizations should work proactively with experts in the relevant domains to recognize and mitigate potential cybersecurity risks. Healthcare professionals can:

Identify risky circumstances: The HHS Office of the Inspector General recently reported that a "large Southeastern hospital" had conspicuous weaknesses in its cyber defenses. For example, multifactor authentication was not enabled on an account management platform, and a mock phishing campaign captured credentials that should have been secure. Cybersecurity experts can identify digital risks and help the practice avoid potential negative events – including those related to civil liability; contract violations; and administrative complaints to governmental oversight agencies. These events can result in administrative investigations – along with highly detrimental and often defamatory social media postings – which can potentially injure the reputation and ongoing financial stability of the practice or institution.

Provide training across the enterprise: Cybersecurity professionals identify AI-driven social engineering as one of their top concerns. A senior leader at the American Hospital Association described "a patient safety-focused culture of cybersecurity" as an organization's "most important defense."

Design in-house patient safety precautions: Distributed denial-of-service attacks can lock legitimate users out of a hospital's computer systems, including its EHRs, presenting a swarm of simultaneous threats to patient safety.

Investigate insurance coverage: Corporate counsel, agents, brokers and liability carriers can help organizations consider the nature, scope and amount of business protection that may be advisable. Developing a comprehensive risk assessment before a crisis occurs is critical to ensuring continuity of professional services and operational integrity in the event of an unforeseen adverse event.

Coordinate with business partners: Healthcare practices and systems, working closely with their insurance carriers, can coordinate with business partners to develop policies and procedures to evaluate and address risks. Periodic audits of office policies can help ensure that protocols are being applied uniformly; are being updated at regular intervals to comply with evolving standards; and are properly and timely documented. Such documentation ensures that the facility can prove with competent and convincing evidence that due diligence was exercised to protect patients and business associates.

The fates of U.S. healthcare organizations and their business partners are linked, so each healthcare system must mount a vigorous cybersecurity defense. **PSN**

Richard J. Cahill, JD, is vice president and associate general counsel for The Doctors Company, part of TDC Group.

YPS Forum expands eligibility to members

The ASPS/PSF Board of Directors in May approved a bylaws amendment, changing eligibility for the Young Plastic Surgeons (YPS) Forum. Participation now increases the maximum eligible age to 45 from 42 – and the maximum years in practice to 10 from eight.

The training pathway in plastic surgery has evolved, with many trainees taking one to three additional years for research, gap years or advanced degrees. As a result, surgeons are entering practice at older ages.

"During my tenure as YPS chair, it has become clear that many highly qualified members enter the YPS Forum later and subsequently have a limited window for meaningful engagement before aging out," notes YPS Steering Committee Chair Ashley Amalfi, MD, Rochester, N.Y. "This has constrained leadership development, continuity and succession planning."

Additionally, not all early-career surgeons engage with ASPS immediately after training due to practice transitions or geographic changes. Expanding eligibility allows the forum to capture these individuals when they're ready to engage and ensures the Society doesn't lose high-potential future leaders due to timing alone, retaining talent in the leadership pipeline for ASPS.

"Updating these criteria is a strategic, forward-looking adjustment that supports ASPS priorities in recruitment, retention and leadership development of new members," Dr. Amalfi says. **PSN**