Privacy during Pandemic:

Where to ease & where to tighten

Diane Evans, Publisher, MyHIPAA Guide
DEvans@MyHIPAAGuide.com

HIPAA is about privacy and security

What to ease and what to tighten during COVID-19

Privacy

is about protecting private health information; ease privacy for higher purposes.

Security

is about keeping healthcare data under lock & key; tighten security in response to new threats.

Crisis Management Objectives

1. Proficiency in new federal directives on privacy
2. Preparedness to thwart COVID-19 hackers
3. Capacity to communicate IT safety practices to staff

New federal directives on relaxed privacy standards

Use professional judgment and good faith to:

- disclose PHI to protect public health & individuals at risk
- see patients via telehealth platforms

Sources: U.S. Office for Civil Rights (OCR) Memo 2/3/2020 and OCR Memo 3/17/2020

Disclose PHI for:

- Treatment coordination
- Protection of public health (i.e., a local health department)
- Protection of individuals at risk
- Family members involved in care

Disclosure limitations

- Stick to the “minimum necessary” standard
- Do not report individually identifiable information to media

Guidelines for telehealth

- No restrictions on patients who can receive telehealth
- No HIPAA penalties for good-faith delivery of care during COVID-19
- Stick to private locations and settings
- Professional judgment applies on types of care via telehealth
- Avoid public-facing platforms such as TikTok and Facebook Live

Source: OCR FAQ for Telehealth during COVID-19

Preparedness to Thwart COVID-19 Hackers

- Know how cyber criminals operate and arm staff with information and security tips
- Practice safe telecommuting to the extent possible

Common hacking tactics

- Phishing attempts, with COVID-19 information as the lure

  emails claiming to come from a trusted source, such as the World Health Organization, designed to induce the user to reveal security information

- Watch where you click!

  emails encouraging users to click on links to scam websites or malicious downloads

Source: Department of Homeland Security

Signs of suspicious activity

- Authority ~ the sender claims to be an official source
- Urgency ~ a sense of need to act quickly
- Emotion ~ the message elicits a sense of panic or fear
- Scarcity ~ the message purports to offer something in short supply

Source: Department of Homeland Security

What those in authority can do

- Keep IT systems updated and monitored
- Respond quickly to incidents
- Require safe telecommuting practices
- Train staff to spot and report suspicious activity

Refer to federal resources titled Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams

Examples of IT system checks

- Ensure Virtual Private Network and other remote access systems are fully patched
- Enhance system monitoring to receive detection and alerts on abnormal activity

Update response plans

- Make sure staff knows to stop activity at the first sign of suspicious activity
- Establish protocol for notifying IT immediately

Safe telecommuting policies & procedures

- Telecommuting presents its own unique challenges
- Address the challenges in policy
- Communicate policy requirements to managers

Source: The National Law Review

Examples of practices to address in telecommuting policy

- Remote access procedures
- Safe practices for transmitting information to the organization
- Protection of PHI in remote locations

Make sure managers understand details such as:

- Remote access procedures
- Transfer of data requirements
- Required safeguards for protecting PHI in remote locations

Educate staff so they can truly be front-line enforcers

- Don’t settle for rote learning to meet official training requirements
- Train staff to recognize suspicious activity
- Strive for a culture of vigilance where protection of PHI is viewed as everyone’s job

Communicating IT safeguards to staff

Benchmarks of success:

- Employees understand that a single misplaced click of a mouse could open the door to a database
- They know the signs of suspicious emails, attachments and links
- They know what to do, and who to contact, immediately

The challenge:

Cultivate situational awareness for everyday vigilance

- Your front-line defense is only as strong as your least attentive staff member who has access to private data
- Make sure staff understands they are keepers of the keys to your organization’s data – and the IT systems that enable delivery of care

Examples of what staff should know

- Never click a link or open an attachment from an unknown sender
- Only visit work-related websites you know
- Don’t click on links to sites you don’t know

Conclusion

- Tight security protects privacy *and* the delivery of care
- No organization can escape the reality of cyber threats
- Small safety measures -- akin to the use of hand sanitizer - can prevent big problems

Source: Landmark industry report on Managing Threats and Protecting Patients