Common HIPAA Violations Quiz: Where Do You Stand?
By Tod Ferran

HIPAA security auditors like me visit practices to poke through every nook and cranny of company policy, procedure, documentation, and network security in a HIPAA security assessment. 99% of the time, we find problems, even in well-established practices employing an experienced and security conscientious staff.

I've used those common blunders to compile a HIPAA violations quiz that office managers, administrators, surgeons, staff, and physicians can easily take during a quick tour around the office.

Take the quiz!
Keep track of your points to determine your overall score.

1. Stand where your patients check in and walk the paths your patients walk. Do you see any PHI (name, address, phone, email, Social Security Number, etc.) anywhere on desks, receptionist counters, computer monitors, or shelves? Remember, many people can read upside down and side-ways, so if it's visible, someone can read it!
Yes: 0 points
No: 1 point

2. Walk around the office and look at every workstation. Are there sticky notes, notepads, calendars, etc. on or under monitors, keyboards, desks, or mouse pads with passwords, usernames, or PHI?
Yes: 0 points
No: 1 point

3. Walk around the office and look at empty workstations. Are there any computers that haven't timed out/logged out?
Yes: 0 points
No: 1 point

4. Read through your company's policies and procedures. Do you have documentation of each employee's HIPAA Privacy and Security training?
Yes: 1 point
No: 0 points

5. Read through your company's polices and procedures. When were employees last formally trained on HIPAA compliance?
0-6 months: 2 points
6-12 months: 1 point
Over 12 months, or unknown: 0 points

6. Does your office have a designated HIPAA Privacy and Security Officer?
Yes: 1 point
No: 0 points

7. Do you have a formal HIPAA Risk Analysis Report and Risk Management Plan?
Yes: 1 point
No: 0 points

8. Do employees share login IDs or passwords? (e.g., all nurses use the same login or password for computer, software, physical access)
Yes: 0 points
No: 1 point

9. Ask a random employee how they would dispose of documents containing PHI.
Shred or burn: 1 point
Throw away or recycle: 0 points

10. If you have any personal mobile devices connected to your office network, is all PHI encrypted?
Yes: 1 point
No: 0 points
We don't have any personal mobile devices connected to the office network: 2 points

Before scoring, let me explain the HIPAA violations that correspond to the questions above.

Sensitive info in plain sight (#1, #2)
PHI stuck on bulletin boards or passwords hastily scribbled on sticky notes are easily seen by office outsiders. What if the nightly janitor used a password he found tucked under a keyboard to login and access, copy, or alter medical records? Luckily, this violation has an easy fix: staff training.

Lack of screensavers (#3)
Even if an office computer or mobile device is timed out, will PHI be displayed if the mouse is accidentally (or purposely) bumped? Train staff to manually lock screens with a password protected screen saver whenever they leave their desk. Even for just a moment. You never know who may be watching.

Untrained staff members (#4, #5)
Policies and procedures aren't just paperwork. They are the blueprint to your practice's compliance plan. All healthcare employees must be formally trained on HIPAA compliance regularly.

Nobody in charge (#6)
When everyone is accountable, no one is. Designating a HIPAA Privacy and Security Officer with the responsibility to ensure HIPAA compliance happens at your practice means it won't get brushed under the rug.

Lack of analysis and planning (#7)
As per HIPAA regulations, entities are supposed to have a formal HIPAA Risk Analysis and Risk Management Plan. Just as policies are the blueprint to company procedures, Risk Management Analysis and Plans are the roadmap to achieve security and compliance.

Sharing login information (#8)
Every staff member should have access to PHI based on business need. Receptionists shouldn't have the same access to PHI as nurses, and nurses shouldn't have the same access as surgeons. Ergo, every person needs a different username and password with access to the minimum information needed to complete their job.

Improper disposal of PHI (#9)

Ensuring PHI is correctly disposed seems like a no brainer, but I wouldn't be writing about it if it weren't a serious issue. The HHS says shredding, burning, pulping, and pulverizing are the only way to destroy paper records. Paper PHI should never be thrown away in a dumpster, recycle bin, or office trashcan.

Using personal devices at work (#10)

It's now common practice for doctors, surgeons, and nurses to use the same mobile device for viewing and sending PHI as they do for making calls, downloading apps, and Internet browsing. What happens if a new app you download contains malware and logs every action your phone makes (including the PHI you viewed earlier that day)? If you must use a personal device at work, ensure the PHI you send or view is encrypted.

Scoring: Let's see how you did!

Add up all your points to discover your score.

0-5 points: Yikes! You really need to work on your HIPAA compliance!
5-10 points: Good start, but you have work to do
10-12 points: Awesome start! You're on your way to HIPAA compliance!

Before you start celebrating your good score (or criticizing your bad score), let me put that quiz into perspective. Those questions only cover 10 of the 535 HIPAA validation points required of entities. Yes, **535**.

Validation is specific evidence needed to support the appropriate implementation of the requirement. For example, enabling a password-protected screensaver is an example of one validation point. Let me break it down even further.

- The Security Rule contains 75 requirements with 254 validation points
- The Breach Rule contains 10 requirements with 26 validation points
- The Privacy Rule contains 72 requirements with 255 validation points

The point is, even if you aced the quiz, you've barely scratched the surface of what is required in HIPAA compliance. I hope you take the questions you failed and work to fix those first. Then, start working on all 535 validation points. For a more comprehensive look into your practice's HIPAA compliance, I recommend discussing your security with an expert.

Tod Ferran (CISSP, QSA) is a Security Analyst for SecurityMetrics with 25 years of IT security experience. He provides security consulting, risk analysis assistance, risk management plan support, and performs HIPAA and PCI compliance audits.