stratx IT

Dawn Meglino

StratX IT Solutions

HIPAA Privacy & Security Officer

HIPAA AND TECHNOLOGY:
WHAT COULD POSSIBLY GO WRONG?

stratx IT
For a happier network.

How safe is your environment?

- ✓ If you look at HIPAA breaches and the HIPAA Wall of Shame, almost always the companies listed had an incomplete Risk Analysis or didn't conduct one at all.
- ✓ A Security Risk Analysis must be conducted annually. By not doing so your organization is blind to potential security vulnerabilities.
- ✓ The network environment needs to be protected with Firewalls, Antivirus, Ransomware, Encryption, Backup and Recovery Plan, etc.,

stratx IT
For a happier network.

Some Current Breaches on the HIPAA Wall of Shame

- ✓ American Collection Agency, New York, 25 million individuals affected. Patient data was impacted in Quest Diagnostic and LabCorp. Hacking/Unauthorized access.
- ✓ Children's Hope Alliance, North Carolina, 4564 individuals affected. Hacking/IT incident from an email.
- ✓ InterMed, Pennsylvania, 11,308 individuals affected. Hacking/IT incident from an email.
- ✓ RCM Enterprise Services, Inc., Florida, 5965 individuals affected. Unauthorized access/disclosure of paper/films.
- ✓ The Center for Facial Restoration, Inc., Florida, 3600 individuals affected. Hacking/IT incident to the network server.

Breaches are not cheap

- ✓ West Georgia Ambulance, Inc. agreed to pay OCR $65,000 and to adopt a corrective action plan. Breach was due to a lost unencrypted laptop.
- ✓ OCR imposed a $1.6 million civil money penalty against Texas Health and Human Services Commission along with a corrective action plan. The breach occurred when an internal application was moved from a private, secure server to a public server. All data was viewable over the internet.
- ✓ Sentara Hospitals (12 acute care and 300 sites) have agreed to take corrective actions and pay OCR $2.175 million. After learning of patient data/records being mailed to the wrong patients, Sentara persisted in improperly reporting the breach.
- ✓ OCR concludes 2018 with an ALL-Time record year for HIPAA enforcement: $28,683,400 in total settlements and judgements.

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Your First Line of Defense?

- ✓ The more training provided and the better educated your staff members are, the more unlikely your Center will suffer from a cyber attack, security incident or breach.

stratx IT
For a happier network.

What steps can you take to make your environment safer?

- ✓ Keep computers clean of any PHI in the documents, downloads, desktop and trash/recycle bin.
- ✓ NO PHI should be saved on the computer's local hard drive.
- ✓ Empty the trash/recycle bin on a regular basis (at least weekly).
- ✓ Do NOT charge cell phones on the business computers.

stratx IT
For a happier network.

What steps can you take to make your environment safer, cont'd?

- ✓ Business Class Firewalls with security subscriptions enabled.
- ✓ Content filtering installed to block any unwanted internet traffic.
- ✓ Encrypt, Encrypt, Encrypt.
- ✓ Software updates and regular patching.
- ✓ Secure Backups onsite and offsite.

stratx IT
For a happier network.

Review user accounts

- ✓ Review user accounts for all operating systems and applications that contain PHI on a regular basis. Ensure all active users are still employed by the Surgery Center.
- ✓ Archived or historic software accounts containing PHI need to be reviewed. Disable inactive users immediately.
- ✓ “Shared” accounts for operating systems and applications containing PHI need to be eliminated. There is no audit trail when multiple users are signing in with the same credentials.

Email Encryption

- ✓ Email encryption is a must for all emails containing ePHI or sensitive data (PII).
- ✓ Any ePHI that is being sent from the Covered Entity via email must be encrypted.
- ✓ If management, staff and doctors are texting ePHI an encryption software tool needs to be installed on the device.
- ✓ If ePHI is encrypted and a ransomware attack occurs, a breach is not reportable: “Safe Harbor”.

Backups/Business Continuity/Disaster Recovery

- ✓ All ePHI needs to be backed up to an offsite location.
- ✓ Mission critical data needs to be backed up (i.e. Server, accounting software, billing and scheduling, etc,.).
- ✓ Business Continuity and/or Disaster Recovery would require the implementation of a redundant virtualized network environment.
- ✓ Scheduled testing and restores should be conducted on a regular basis.

stratx IT
For a happier network.

Are vulnerability scans necessary?

- ✓ HIPAA compliance rules indicate that vulnerability scans for systems and networks are required. The frequency of the scan is up to the Covered Entity, but should be done at a minimum annually.
- ✓ Vulnerability scans identify areas on the firewalls configuration that could potentially let the “bad guys” onto the Centers’ network.

stratx IT
For a happier network.

Don’t Forget Physical Securities

- ✓ Physical securities are a HIPAA requirement to ensure equipment is secured, locked server racks are in place, computers locked when not in use, and all patients and visitors are escorted through the Surgery Center.
- ✓ Clean Desk Policy – lock up or put away any PHI in drawers or cabinets. Do not leave papers containing PHI on an unattended desk, counter or fax machine.
- ✓ Documents containing PHI should not be accessible to the public, or left unsecured in the Surgery Center. The Clean Desk Policy must be in effect for after hours.

Don’t Forget Physical Securities

- ✓ Retention periods need to be set for older charts and papers containing PHI.
- ✓ Limit physical access in the Surgery Center wherever possible. Change locks, codes, disable badges immediately upon a termination, resignation. Allow limited access depending on a staff member’s job duties.

Are there any Penalties for violations of HIPAA?

- ✓ Four categories of violations and four corresponding tiers of civil monetary penalties:
  1. Person did not know (and, by exercising reasonable diligence, would not have known) of a violation;
  2. Violation was due to reasonable cause, and not willful neglect;
  3. Violation was due to willful neglect that is timely corrected; and
  4. Violation was due to willful neglect that is not timely corrected.
- ✓ HHS has proposed increases for civil money penalties (CMP) for HIPAA violations in accordance with the Inflation Adjustment Act. At this time increases have not been made official and are pending.

stratx IT
For a happier network.

Useful Websites

- ✓ The Office for Civil Rights - https://ww.hhs.gov/ocr
- ✓ National Institute of Standards & Technology - https://www.nist.gov
- ✓ OCR website for HIPAA Professionals - https://www.hhs.gov/hipaa/for-professionals

Dawn Meglino
dmeglino@stratxit.com