Codify
BY AAPC

Eli's Rehab Report

HIPAA Risk Assessment: Update Your Software Or Pay The Price

Tip: Tailor security policies to the actual information security infrastructure you have in place.

Whether you provide inpatient rehab or outpatient rehab or are a private therapist, patient health information privacy is an area you can't afford to ignore. The **HHS Office for Civil Rights** (OCR) has slapped a $150,000 fine on **Anchorage Community Mental Health Services** (ACMHS) following a breach of 2,743 individuals' ePHI, according to a December announcement.

ACMHS is a five-facility behavioral healthcare organization based in Anchorage, Alaska. It will have to pay the settlement and adopt a corrective action plan to fix deficiencies in its HIPAA compliance program. Also under the Resolution Agreement, ACHMS must report to OCR on the state of its compliance for the next two years.

OCR attributed the breach to ACMHS' failure to implement good security processes and regularly update their IT resources with patches, as well as the fact that it was running outdated, unsupported software. Here's what you can learn from this breach.

Don't Take a 'One-Size-Fits-All' Approach

Problem #1: OCR's investigation revealed that ACMHS adopted sample Security Rule policies in 2005, but didn't follow them. "Simply having in place template Security Rule policies and procedures is insufficient to satisfy the requirements of the HIPAA Security Rule and to ultimately secure ePHI," warned Seattle-based attorney **Elana Zana** in a blog post for **Ogden Murphy Wallace Attorneys.**

You need to tailor security policies to the actual information security infrastructure you have in place at your organization.

"The ACMHS settlement underscores that Security Rule compliance cannot be accomplished with a one-size-fits-all, 'check the box' approach," noted Boston-based attorney **Kate Stewart** in a recent analysis for the law firm **Mintz, Levin, Cohn, Ferris, Glovsky and Popeo.**

Remember: The Security Rule allows flexibility when choosing which tools to use to protect ePHI, but requires you to actually evaluate your infrastructure to make these decisions, Zana stressed.

Make Security Risk Assessment Your Best Friend

Problem #2: ACMHS failed to identify and address basic risks by conducting a thorough risk assessment, and did not implement security measures to reduce risks and vulnerabilities to its ePHI, OCR charged.

You must evaluate your security policies and procedures, and conduct a security risk assessment on your actual system, at least annually, Zana advised. The process of drafting the security policies and procedures, as well as conducting the security risk assessment, will help you to identify vulnerabilities, evaluate security options, and ultimately safeguard your ePHI.

"OCR has repeatedly emphasized the importance of conducting risk assessments and continuing to update and revise risk assessments based on new threats," Stewart noted. This was a key takeaway from the Joint OCR/NIST HIPAA Security Conference held in September, and was highlighted by OCR's release of a Security Risk Assessment Tool earlier this year (www.healthit.gov/providersprofessionals/security-risk-assessment).

Patch, Repair & Update

Problem #3: ACMHS failed to "ensure that firewalls were in place with threat identification monitoring of inbound and outbound traffic, and supported and regularly updated with available patches," OCR stated.

"Like Community Health Systems, which reported a breach of 4.5 million patient records due to Chinese hackers targeting a 'heartbleed' vulnerability, ACMHS is finding out the hard way the importance of software patching and updating," Zana said. "Staying up to date on security patches and software updates is not an easy task, but an important one considering that hackers are exploiting these vulnerabilities."

"Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis," OCR Director **Jocelyn Samuels** said in the announcement. "This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."

Note: Read ACMHS' Resolution Agreement at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf.