What Can We Learn About HIPAA From Phoenix Cardiac Surgery?

Phoenix Cardiac Surgery probably never thought they would be a poster child for HIPAA safeguards, but this 5-physician cardiothoracic practice in Prescott, Arizona has become famous for something no medical practice wants to be famous for – not protecting their patient information.

Today's HHS Press Release reads as follows:

HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards

Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona, has agreed to pay the U.S. Department of Health and Human Services (HHS) a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the protected health information of its patients.

The settlement with the physician practice follows an extensive investigation by the HHS Office for Civil Rights (OCR) for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

The incident giving rise to OCR's investigation was **a report that the physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible**. On further investigation, OCR found that Phoenix Cardiac Surgery had implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules, and had limited safeguards in place to protect patients' electronic protected health information (ePHI).

“This case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules,” said Leon Rodriguez, director of OCR. “We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity.”

OCR’s investigation also revealed the following issues:

- Phoenix Cardiac Surgery failed to implement adequate **policies and procedures to appropriately safeguard patient information**;
- Phoenix Cardiac Surgery failed to document that it **trained any employees on its policies and procedures** on the Privacy and Security Rules;
- Phoenix Cardiac Surgery failed to **identify a security official and conduct a risk analysis**; and
- Phoenix Cardiac Surgery failed to obtain **business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.**

Under the HHS resolution agreement, Phoenix Cardiac Surgery has agreed to pay a $100,000 settlement amount and a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules.

Individuals who believe that a covered entity has violated their (or someone else’s) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsu

rgery_agreement.pdf

Additional information about OCR's enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

What Can We Learn?

1. **You won't escape the notice of the HHS just because you are a small practice.** Every practice, hospital, facility, healthcare entity and anyone that has access to Protected Health Information (PHI) must be compliant with the HIPAA Privacy and Security Rules.
2. **Patients are paying attention and want their information protected!** Patients will not hesitate to report a practice if they feel their privacy is being breached. Let your patients know that you take their privacy seriously and what you are doing in your entity to protect their privacy.
3. **Physicians are not exempt from responsibility.** Most physicians do not want to use the hospital or practice network email – they want to use their personal Gmail, Yahoo, Hotmail or AOL account for office business. This is a bad habit. Emails to and from the physicians announcing meetings and reminding them of tasks are fine, but it is easy to forget and use personal email to hand off patients, discuss appointments and ask for refill approvals. Non-secured email services are NOT the right way to send any patient information.
4. **Understand your technology.** This is why the risk assessment is so important – you must identify any process or technology you are currently using that has the potential for PHI to be accessed inappropriately. Understand and mitigate your risk!

;

Resources

Health Information Privacy for For Small Providers, Small Health Plans, and other Small Businesses here

Summary of the HIPAA Privacy Rule

Summary of the HIPAA Security Rule

There are lots of resources available from the AMA, your state medical society, your specialty society and MGMA. There are also a number of consultants specializing in this area.

Don’t forget to talk to your IT person – they should be looking after your best interests and helping you with privacy and security issues.

For practices looking for a secure place to share files and collaborate on documents with encrytpted upload and download capability, please consider FileConnect, a product brought to you and supported by Manage My Practice. For more information, call Abraham at 919-370-0497 or email him at abe@managemypractice.com.