Online calendar exposes patient appointments on Internet

Who can see your patient appointment information?

Phoenix Cardiac Surgery (PCS), a non-Providence provider, has agreed to pay the Department of Health and Human Services (HHS) $100,000 for posting patient information on the Internet in violation of HIPAA.

According to HHS, over several years, the two-physician practice put patient confidential information at risk by:

- Posting more than 1,000 separate entries of clinical and surgical appointments on a publicly-accessible, Internet-based calendar
- Transmitting electronic Protected Health Information (ePHI) from an Internet-based email account to employees’ personal email accounts on a daily basis.

PCS also failed to document HIPAA training for any of its employees or to obtain a business associate agreement with its Internet-based email and calendar services.

Providence practice

While it is tempting to take advantage of Internet-based applications to improve productivity, usually these tools do not protect the privacy and security of patient information. Providence has fielded requests from physician practices to use Internet-based tools such as Google Calendar, and we have turned down these requests because their use puts our patients’ privacy at risk and does not comply with the HIPAA privacy and security rules.

When you and your colleagues work with confidential patient information, please follow these practices:

- If you must travel with patient files, take only the minimum necessary information for the care of those current patients.
- When you are off-site, access patient files securely, such as through a Virtual Private Network (VPN).
- Remember Providence policy specifically prohibits “emailing or otherwise sending confidential information to a personal email account or Internet storage service.”
- Contact your IS department if you have any difficulties using secure access or SharePoint tools.