MDS Alert

Reader Questions: Beware HIPAA Rules for Electronic Faxes

Question: Our facility sometimes works with other institutions that use electronic faxing for medical records. Do you have any advice on the best way to protect our residents' privacy and protected health information (PHI)?

Georgia Subscriber

Answer: Once a fax becomes electronic, it is considered electronic PHI (ePHI). When you change the format, you're required to develop proper access controls so that only authorized users can see that document.

Your organization should store faxes on a central server where users have the ability to know that the intended fax recipient actually received the information. Ensure that the server is well secured and protected. If you're using an outside vendor, make sure the vendor is HIPAA-compliant.

"The covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules," HHS Office for Civil Rights (OCR) says.

Don't forget: You're responsible for protecting outbound faxes, too. Establish a validation procedure, so that if, say, a resident's representative asks you to fax them something, you can determine whether it is an authentic request.

Tip: It's critical that you have procedures in place to ensure that you send faxes to the right place. Additionally, when you receive an electronic fax, be sure it has the same protections as the rest of your ePHI.