Ensuring Remote Coding Compliance

Save to myBoK

By Angie Comfort, RHIT, CCS

More and more HIM department managers are turning to remote coding. However, before implementing this staffing model, managers must answer several questions regarding the privacy and security of patient information, including:

- What are the compliance risks?
- How will privacy and security be achieved?
- How will the remote employee be held accountable for the security of patient health information?

Remote coding can create serious compliance risks because the organization loses significant control over its privacy and security practices. Some areas for concern are insufficient security of medical records and inadequate destruction of patient health information.

Organizations must maintain strict policies and procedures for remote coding, and remote coders must acknowledge them before being allowed to work remotely. In addition organizations should create a security checklist, telecommuting agreement, and confidentiality statements for remote coders and conduct an annual review of the code of conduct.

Remote Coding Policies and Documents

One of the first things an organization should do before implementing a remote coding program is create a remote coding/telecommuting policy. The policy should include everything from who coders should call for equipment issues to what should happen if they need to report a compliance issue.

When putting the program together, it is important to lay out all the rules and guidelines that remote coders need to follow. Organizations should also ensure that coders are aware of and understand all aspects pertaining to remote access and everything that will be required of them as remote coders.

In addition, the HIM manager should work with the information systems manager to make certain all areas from a system perspective are covered and create a security checklist to ensure privacy and security compliance. The checklist should cover the organization's policies and guidelines pertaining to remote coding and access, identification and authorization, access control, auditing, integrity, physical security, security administration, education, awareness, and enforcement.

The checklist should address the following questions:

- Is a remote access security policy in place?
- Are there automatic time-out or lock-screen capabilities on the remote site equipment to control access during periods of nonuse?
- Are user sign-ons restricted to a single remote connection to the organizational network?
- Do audit trails follow remote users as if they were inside the physical organization?
- Is there a clear process for returning organization-owned equipment upon an employee's termination?

A remote coding agreement is another key element for maintaining remote coding compliance. It should contain statements to ensure that the coder knows what the organization expects from the employee in the remote coder role.

The employee and manager should sign the agreement to attest that each party understands the document. It may be appropriate to have these forms signed and updated on an annual basis.

The following is an excerpt from a sample telecommuting agreement:

- I have read and understand the attached Telecommuting Policy and agree to the duties, obligations, responsibilities, and conditions for telecommuters described in that document.
- I agree that, among other things, I am responsible for establishing specific telecommuting work hours, furnishing and maintaining my remote work space in a safe manner, employing appropriate telecommuting security measures, and protecting company assets, information, trade secrets, and systems.
- I understand that telecommuting is voluntary and I may stop telecommuting at any time. I also understand that the company may at any time change any or all of the conditions under which I am permitted to telecommute, or withdraw permission to telecommute.[1]

The Remote Coding Workspace

Once the policies and procedures have been developed and HIM and IS have completed the security assessment, remote coders must understand how to make their remote workspaces secure.

When designing the work area, it is more secure to face the computer screen away from doorways and windows to prevent someone from viewing patient health information. Entertaining guests, children, or spouses in the work area while accessing patient health information is not appropriate.

Remote employees must never leave computers available for access when they are not present. They should get into the habit of locking the computer when not working, and log-ins should time out after a period of inactivity.

It is very important to make certain that all patient health information is safe and secure in the remote coder's office area. Hard-copy records sent from the facility to the employee need to be stored in a locked desk drawer or filing cabinet until the records can be properly disposed of. The disposal process should be part of the remote coding policy and procedures.

An organization should never send remote coders original medical records due to compliance risks, including the loss or destruction of the records while outside of the organization. If the organization needs to send copies of patient files, it would be more compliant to send them on an encrypted CD or DVD rather than paper. The encryption will protect the patient's information against access if the disc is misplaced or lost during transit.

There are many risks associated with a remote coding program. However, with the proper secure equipment and private networks, assistance from IS in making the transition, and training of the remote employee, a successful program can be achieved and well received.

Note

[1] Fletcher, Donna. "Telecommuting." February 1999. Available in the AHIMA Body of Knowledge at www.ahima.org.

Angie Comfort (angie.comfort@ahima.org) is a professional practice resource director at AHIMA.

Article citation:
Comfort, Angie. "Ensuring Remote Coding Compliance" *Journal of AHIMA* 83, no.4 (April 2012): 56-57.