Make Your Telecommuting Program HIPAA Compliant (HIPAA on the Job)

by Margret Amatayakul, RHIA, FHIMSS

An increasing number of healthcare workforce members are telecommuting. As transcriptionists, coders, customer service representatives, and others are working from home, many providers are weighing the benefits against potential privacy and security risks.

Who Is Working from Home?

There are two general types of home-based workers: those contracted by a provider and those employed by a provider. Although the organizational relationship may make no difference in terms of what the risk is and how it should be mitigated, the relationship does determine how a provider controls the risk.

For the contractor, the provider must have a **business associate agreement** to establish a contractual arrangement for safeguarding protected health information. The provider generally does not directly evaluate the home-based worker of the contractor. However, the guidelines offered here could be used by the contractor to establish safeguards and for the provider to establish contractual obligations.

Specific types of workers who may work from home may be considered narrowly or broadly from a HIPAA perspective. Transcriptionists are perhaps the most common home-based workers. Increasingly, coders are looking to work from home as well. Other groups of home-based workers are business office customer service representatives and staff who perform preregistration, eligibility verification, and precertification.

In interpreting the home-based worker role more broadly, however, one could include virtually anyone who has remote access to protected health information, brings work home on floppy disks or laptops containing protected health information—even only occasionally—or uses personal
e-mail to communicate with patients.

What Protected Health Information Do Telecommuters Need?

Each type of home-based worker has different needs for protected health information. These needs already determine the feasibility of performing the task at home and should be carefully evaluated against minimum necessary criteria and potential for de-identification.

HIPAA should help us challenge current thinking about what and how all protected health information is used and disclosed. For example, home-based or not, transcriptionists and coders may actually not need patient identity to transcribe or code records. From a practical perspective, however, it may be difficult to de-identify the dictation or the record content, but this is becoming easier with new technology. Some systems today are capable of randomly assigning a document number to dictation that can be converted back to the medical record number when the transcription is transmitted back for filing.

Document scanning systems can be programmed to replace a patient identification bar code with a randomly assigned number. Not only would this remove patient identity from the documents used by the coder, but it would serve as a check on the contents of the paper chart to ensure that all relate to the same patient.

Employees who occasionally take work home on floppy disks would rarely, if ever, need protected health information. However, if there is identifying information in spreadsheets or databases that are used for processing at home, take steps to separate the identifying information from the information to be processed where possible.

Measures such as assigning a code to replace the patient name and medical record number or deleting an identifying column on a spreadsheet do not fully de-identify the patient, according to the 19 data elements required by HIPAA for de-identification. These measures, however, go a long way toward addressing minimum necessary use requirements and protecting transmission of data to remote locations when the worker would ordinarily have access to patient identity.

Such de-identification, however, does not apply to all who may work remotely. For example, physicians who may access the hospital system or their office system would need the identity of the patient. Visiting nurses could also be considered home based even though the patients' homes they visit are not their own. Other workers, such as customer service representatives, may also need patient identity—both to gain access to information to respond to requests as well as to validate with whom they are speaking. While de-identifying information used in these circumstances is not possible, steps recommended for all telecommuters can be used to better protect individually identifiable health information in these circumstances.

What Are the Risks at Home?

Many risks in the home environment are the same as in the provider setting, but the risks tend to be intensified. While most HIM departments, business offices, and other such operational areas generally are not open to the public, there is a small risk of coworkers who do not have a need to know having access to protected health information. This risk is further minimized on site by the fact that these persons are members of the work force, have received privacy and security training, and have agreed to abide by the policies of the organization under penalty of sanctions up to and including termination. Homes are not areas where members of the "public" have great access, but persons who may visit the home are not under the same obligations as coworkers on site. In the home, there is significantly greater risk of casual observation or overhearing of protected health information by persons not in the employer's work force.

Unscrupulous workers can exist both on site and at home. When on site, however, there are usually fewer opportunities to divert, alter, or destroy information than in a home, where there is no other person to oversee what is being done to the information. In the home environment, transcribed documents, coded encounter forms, and other forms of protected health information can be saved to floppy disks, printed and retained in hard copy, or saved to alternative hard drives or servers. There are also greater risks of errors occurring at home, where there is not direct access to technical support. These problems can result in loss of data, misrouting of information, or accidental access by a person who is not a member of the provider's work force.

Finally, connectivity is an issue for telecommuters. Most security experts believe that the greatest threat to protected health information is still internal—that is, accidental or intentional misuse or disclosure by a member of the work force (whether on site or at home). There is, however, greater possibility of wire tapping, service disruption, or mail interception when connecting from the single point of a home. The courier who routinely transports documents from the home to the provider could be secretly copying contents or gaining unlawful access to the information contained in the documents being transported.

How Can I Achieve Security and Privacy Compliance in the Home?

There are three key steps to providing security and privacy protections for telecommuters. The first is to **hire employees or engage contractors who have been adequately screened** and with whom there is regular privacy and security communication. Out of sight should not be out of mind. Know who is performing the work and how the work is being performed. Every telecommuter should receive privacy and security training, regular updates, and the same—or greater—level of awareness building as those on site. For regular telecommuters, this may include random site visits, e-mail, telephone calls, or other means to provide communications. This not only directs communications to the telecommuter, but also permits them to communicate any concerns they may have.

A second key step is to **ensure that the environment is suitable to afford protections**. For members of the work force who take work home only occasionally or connect remotely for only part of their time, ensure that they too have been appropriately trained and agree to follow appropriate safeguards. The picture of the physician accessing patient information while eating breakfast with the family may be endearing, but it is not necessarily the ideal image of privacy. Not only should the telecommuting environment be ergonomically appropriate and conducive to productivity, but physical and technical safeguards should be provided. Each telecommuting function will have its own set of technical features that must be considered. In addition to these, however, "Sample Telecommuter Safeguards Checklist" is a good place to start for any form of telecommuting.

The third factor is contractual. Even if the telecommuter is an employee, it is advisable to **have an agreement with the facility concerning ownership and use of equipment and rights to information**. When contracting with a service, the provider may want to include in the business associate contract how the contractor ensures that its work force is trained, information is protected, and the legal obligation to conform to requirements. "Sample Telecommuter Obligations" identifies elements that should be included in a telecommuter's agreement or contract. These would be in addition to the elements required by HIPAA for the business associate contract (see the AHIMA Practice Brief "Letters of Agreement/Contracts (Updated)" published in the June 2001 *Journal of AHIMA*).

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Sample Telecommuter Safeguards Checklist

This list represents only a sample of approaches to structuring a telecommuting security policy. For a complete list, see the AHIMA Practice Brief "Telecommuting" published in February 1999 and available online at www.ahima.org.

___ Work location in separate room or room unused by others during work time
___ Private area for connectivity/remote access and/or telephone conversations
___ Separate phone line if remote connection to provider or contractor
___ Smoke detector/alarm present and functional in area of workstation
Date last checked:_____

___ Fire extinguisher near work area and accessible
___ Power surge protector available for workstation
___ Equipment out of direct sunlight and away from heaters
___ Lock on work area door/workstation
___ Workstation password protected

Sample Telecommuter Obligations

This list represents only a sample of possible telecommuter obligations. For more details, see the AHIMA Practice Brief "Telecommuting" published in February 1999 and available online at www.ahima.org.

___ Signed confidentiality agreement or business associate contract in place
___ Telecommuter will commit to participating in training sessions and achieve required competency on privacy and security standards at least annually
___ Telecommuter will be accessible by phone and/or e-mail during designated work time
___ Telecommuter will make work area available for inspection during designated work time
___ Workstation will not be used for any other purpose or by any other person except designated staff of provider or contractor (provider or contractor will ideally own equipment)
___ Workstation will not include capability to save to local media (backups will be performed by provider and/or contractor)
___ Workstation will not include capability to print, fax, or otherwise transmit information except to designated site

Article citation:
Amatayakul, Margret. "Make Your Telecommuting Program HIPAA Compliant." *Journal of AHIMA* 73, no.2 (2002): 16A-C.