Ensuring Privacy and Security in Home Health

by Barbara Demster, MS, RHIA, CHCQM

Every healthcare provider must customize its privacy and security program to fit its unique setting and needs. How an organization maintains its records (analog, paper, electronic, or mixed modes) drives its privacy and security procedures. While regulations provide the basic requirements, the implementation details vary among organizations because of size and complexity, type and scope of services, physical geography, degree of electronic implementation, and technological advancement or limitations. Home healthcare is no different in being subject to these regulations. The differences lie in its unique exposures and risks.

From the privacy and security perspective, the home health agency central business office may be comparable to any healthcare office setting, including the administrative, physical, and technical aspects of security. An appointment reminder left on a home answering machine should be crafted to protect the individual's privacy, whether it originates from a hospital admissions department, physician's office, or a home health agency. However, as the home health staff moves into the home, special privacy and security issues emerge. Many issues, while not unique to healthcare, take on a greater degree of importance in the home care setting.

On the Road with Records

Healthcare institutions have a long-ingrained policy that an original record should not leave the building except under legal directive. Home health turns this standard on its ear. Home health staff members carry personal health information (PHI) to and from a client's or patient's home. They travel in personal cars or on public transportation. At the end of the workday, PHI may travel to the grocery store, a soccer game, and to staff homes overnight. The potential for PHI exposure to the patient's and staff members' family, friends, neighbors, and acquaintances increases. Management must address these risks through administrative, behavioral, physical, and technical privacy and security policies, procedures, and practices.

In-home Risks

Privacy and security pitfalls await home health staff in a client's home. Some issues to be anticipated are discussed below.

The home record. Home health staff should have a clear understanding of:

- How much and what type of information should be included in the home record: minimum necessary is always the rule of thumb.
- How to document the care of multiple clients in one home and the health status of nonclient family members also living in the home.
- How to protect the record from unnecessary exposure in the home.
- Where to keep the record in the home.
- What happens to the record when the account is closed.

Home health staff demeanor. Staff training should provide suggested behaviors for the in-home environment. These may include scanning the environment on arrival for potential privacy exposures and suggesting potential remedies such as voice modulation, door closure, use of privacy shields, and asking people to exit during care.

Presence of others in the home. The environmental scan should include who in the home should or should not have access to PHI, including family and visitors. Staff members need to understand the importance of providing the patient the opportunity to agree or object to whom information may be disclosed. HIPAA allows this type of interchange to be done orally. For example, a patient may say, "It's okay to talk with my spouse but not my kids." Procedures should be clear and training thorough on levels and types of disclosures, including incidental disclosures.

Using home resources. Training should cover other means of inadvertent PHI disclosure such as using the patient's home phone to contact the next appointment or to report to the office; discarding worksheets containing PHI in the patient's waste basket; or using the patient's home fax machine or computer to transmit information.

What happens in Vegas stays in Vegas. Access to personal information and family dynamics skyrockets when care is provided in the home. As in institutional care, staff must not carry tales home or into the community. Idle chatter can devastate families. Staff must maintain a professional relationship with their clients and avoid becoming too comfortable with the patient or family, which can blur boundaries of professionalism and friendship that are more clearly delineated in the institutional setting. Agency policies and training must ensure awareness and vigilance in this area.

Recommended Actions

Home health agencies should outline procedures for staff that include:

- Developing a comprehensive definition of PHI with examples appropriate to the home health business.
- Designing a PHI data flow from creation to ultimate disposal. Include where and how data travel and the media used at any given stage of the life cycle (paper, electronic, oral).
- Performing a risk assessment to identify areas of exposure and creating a foundation for management policy and procedure decisions.
- Developing written policies and procedures to ensure the privacy and security of PHI throughout its life cycle. In addition to the standard policies and procedures, home health agencies should pay close attention to policies on:
    - Uses and disclosures including minimum necessary, incidental disclosures, obtaining permissions, and how to manage others in the home environment
    - Incident reporting and how to preserve evidence, including how to handle suspected abuse
    - Documentation of multiple clients in the home
    - Providing a secure PHI environment in the home and on the road, including adequate data protections during transmission and at rest, protection of portable electronic equipment such as a laptop from weather extremes, as in hot cars in the summer
    - Use of client home resources such as telephones, home computers, faxes, and copiers
    - Securing PHI in the home office
    - Proper methods for disposal of records and working documents, as well as mobile devices
- Developing an ongoing training program with appropriate tools for all staff.
- Performing regular monitoring or auditing of privacy and security practices.
- Enforcing the policies and procedures-it is good business.

Barbara Demster *(bdemster@benchmarkconsulting.com) is chief compliance and privacy officer for Benchmark Consulting Services in Atlanta, GA, and coeditor of the HIMSS Privacy & Security Toolkit.*

Article citation:
Demster, Barbara. "Ensuring Privacy and Security in Home Health" *Journal of AHIMA* 78, no.1 (January 2007): 62-63.