NEWS & VIEWS

A Complimentary Newsletter from Med-Net Concepts, LLC
and its Network of Independent Affiliated Companies

Volume 4. Issue 4
April 2018

In This Issue:

Med-Net Concepts, LLC

Ensuring the Privacy of Residents through an Effective Privacy Compliance Program

By:
Louise Lindsey, Editor

Persons living in areas where there are Amish communities for the most part are sensitive to the fact that these people have very strong religious beliefs regarding being photographed. Yet, it is not uncommon for a tourist to snap a picture of these people who in their eyes live and dress so differently from the general population. To many people, this seems like "no big deal" and "those Amish people are just weird and out of touch." But, would a closer look would say that a snapshot obtained without permission is an invasion of privacy?

Although there is not much chance that an Amish person would file a civil lawsuit against the photographer because of their religious beliefs, they could legitimately do so.

In today's world of identity theft, electronic recordkeeping and social media, privacy is a concern for all people. Invasion of privacy is categorized into four main forms and all of them can result in a civil lawsuit. The following are the four invasion of privacy forms with some examples:

- Intrusion of Solitude-intercepting phone calls, peeping, taking photographs without the person's knowledge or consent;
- Appropriation of Name or Likeness-using another person's name or likeness (photograph or video);
- Public Disclosure of Private Facts-distributing private information that is not of public interest or part of public records and
- False Light-publishing false or misleading information.

To respect and protect the privacy of the residents in their care and avoid the costly consequences that may accompany reportable, non-compliance incidents, a healthcare provider must have a comprehensive privacy policy in place to address all the applicable aspects of respecting a resident's dignity and privacy and securing their protected health information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) oversees how Protected Health Information (PHI) is used and how it may be disclosed. PHI is made up of any information from which the identity of an individual can be determined. Some of the most obvious information is the individual's name, date of birth, social security number, diagnosis or a medical record number. Other information that falls into the PHI category involves a person's health and healthcare history. Also, PHI can be any information that a healthcare provider learns while providing care for the person. It should be noted that a healthcare provider may only disclose PHI information for purposes of treatment, payment or healthcare operations. Any other disclosure requires the healthcare provider to obtain permission to do so from the individual or their duly appointed responsible party.

Here are some important aspects of a Comprehensive Privacy Program that can help to ensure a facility's proactive response to privacy regulations.

A Designated Privacy Officer

The Privacy Officer is given the responsibility for the general oversight and implementation of the Privacy Program and the day-to-day privacy issues and concerns. The Privacy Officer is charged with enacting preventative measures that include education and the procedures to ensure that the facility's residents' Protected Health Information (PHI) is secure and not inappropriately disclosed. The Privacy Officer is directly involved with investigations of potential breaches and the reporting of any confirmed breaches. Note that the Compliance Officer often also serves as the Privacy Officer, since the requirements are similar.

An important aspect of the Private Officer's job is to make sure that staff understand the importance of not disclosing a resident's PHI inadvertently or overtly by discussions in public places (elevators, lobbies, cafeterias or off premises, etc.), in front of persons not entitled to such information or on social media sites.

The Privacy Officer needs to be knowledgeable about HIPAA regulations. This information can be learned through Med-Net Compliance training that is found at: https://www.mednetcompliance.com/

A Well-Developed Privacy Oversight Committee

The Privacy Committee assists the Privacy Officer with the implementation, coordination and ongoing support of the Privacy Program. The Committee works along-side of the Privacy Officer to maintain oversight of privacy issues and concerns and to manage investigations and corrective actions when issues arise. The Privacy Committee will meet on an as-needed basis to review any privacy concerns and alleged breaches, and work with management to develop, review and approve policies and procedures to promote compliance with the Privacy Program.

Development and Implementation of Policies and Procedures

The Privacy Manual provided by Med-Net is comprehensive and includes all the policies and procedures pertaining to the numerous privacy issues. It describes how potential privacy breaches should be investigated and resolved. These policies and procedures provide specific guidelines for staff performance to prevent potential breaches of protected health information.

Training and Education of Employees about HIPAA Requirements

All employees bear responsibility in the process of ensuring that protected health information is only used and disclosed appropriately. This requires that all employees receive education and training that is appropriate for their jobs. An effective privacy training and education program includes:

- Detailed information about the company's privacy program.
- Orientation for newly hired employees that includes privacy-specific education.
- Privacy training on a regular and ongoing basis.

Business Associate Agreements

The Health Information Technology for Economic and Clinical Health Act (HITECH) extends the HIPAA regulations impacting the confidentiality required of healthcare providers onto their business associates. This means that all vendors and contracts that have access to Protected Health Information (PHI) must receive a copy of a company's privacy plan and they must be informed in writing about their expected compliance to HIPAA's Compliance and Ethics Program. Additionally, these vendors and contractors must sign and return an agreement that defines and explains their responsibilities for not disclosing protected health information.

Anonymous Reporting System (Hotline)

A successful privacy program relies on the ability of personnel to openly and freely communicate issues of concern to their supervisors, the Privacy Officer and the Privacy Committee. It also must be committed to the developing and supporting of any and all lines of communication in its effort to detect, address and prevent

privacy breaches, including the provision of a method for reporting anonymously. The Compliance Hotline provides a way for anyone (including personnel, residents, family members, visitors or even someone who happens to enter the building) to report any perceived compliance breaches. The Hotline is available 24 hours a day, 7 days a week. It provides an individual the freedom to speak candidly. Through a call on the Hotline, any perceived violation can be uncovered and resolved immediately.

How to Respond to a Privacy Breach

The definition of a privacy breach is any use or disclosure of Protected Health Information that is not permitted. Awareness of a privacy breach can come from a variety of sources. It may be a confidential report made to the Privacy Officer, a notification from a business associate or it may come through the anonymous reporting system (Hotline).

The procedure for responding when a potential breach is discovered involves the Privacy Officer who must conduct an initial review and a comprehensive risk assessment of the alleged breach no more than 30 days after the suspected breach is reported. If the Privacy Officer determines that the allegation was not a breach, then specific and clear documentation about the investigation and any conclusions should be maintained. There is no need to continue the investigation at that point.

If the Privacy Officer determines that a breach occurred, it will be reported to the Privacy Committee for review, corrective action and applicable, timely reporting of the breach to affected individuals and the Department of Health and Human Services.

Don't Forget to Address Social Media/Cell Phones/Video Cameras and Artificial Intelligence Devices

Just in the last year there have been numerous instances reported in the news media about photographs of residents taken by staff and then posted on social media outlets like Facebook, Twitter and Snapchat. The postings on Facebook are more easily discovered but photos taken by a cell phone and sent to friends and acquaintances via Snapchat are harder to find and yet they all represent an invasion of a resident's privacy. Prevention lies in the development, implementation and monitoring of a social media/cell phone/video camera/artificial intelligence device privacy policy. This policy also needs to fall under the oversight of the facility's Privacy Officer and its Privacy Committee.

This policy should be written-up and given to all employees (both new hires and longer-term), monitored and reviewed on a regular, periodic basis to ensure that there is a clear understanding that even a "so-called" happy picture of a resident is not acceptable.

Here are some things that administrators can do to ensure they have an effective Privacy Plan regarding Social Media/Cell Phone/Cameras and Artificial Intelligence Devices:

- Provide all staff with media privacy training.
- Monitor the policy but be knowledgeable about the law.
- Pull from your other policies and outside regulations.
- Stay on top of advancing technology and keep your policy current.
- Be consistent in the application of the policy.

Staff are extremely important in all aspects of compliance and especially as it relates to issues involving privacy. A staff that is proactive and diligent in their compliance responsibilities can greatly enhance the effectiveness of a Privacy Plan by:

- Bringing-up ideas and suggestions for improving the plan.
- Becoming familiar with the facility's policies and procedures regarding privacy.
- Erring on the side of caution when it comes to sharing on social media.
- Reporting what you see that is inappropriate.

For more information regarding this article, call 609-454-5020 or email info@mednetconcepts.com.

Med-Net Concepts, LLC Affiliates

Med-Net Compliance, LLC

Med-Net Healthcare Consulting, LLC

Med-Net IPA, LLC

Med-Net Rehabilitation Solutions, LLC

STAY CONNECTED