HIPAA, Privacy and Care of Church members

The information below appeared on a forum for ChMS users in response to a question concerning concerns that a certain church administrator was too restrictive in releasing church member information through the church office. The response below by another forum reader is very helpful in evaluating policies and procedures for the privacy of information in the church office

8/4/2014

As posted by forum participant:

Some of our older Disciples from rural areas remember a time that the names of hospital patients were listed in the local newspaper and even announced on the local AM radio station. Much has changed in healthcare over the past few decades including a greater emphasis on patient privacy and confidentiality. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) set standards for confidentiality that had been emerging in many states, in medical ethics and on the Federal level for a couple of decades before that law was enacted. This law covers healthcare entities including physicians, nurses, hospitals and insurance companies. It does not affect churches however individual church members who are healthcare professionals or hospital volunteers could be subjected to fines.

Even though HIPAA does not apply to churches, the church should ensure privacy of it members out of respect for them. We need to balance our commitment to pray and live in community with one another with a desire to respect information and issues a church member might not want to share with the community of faith or the larger community. The following are some best practices to ensure privacy is protected.

1. If the church has any type of medical entity in its building that receives insurance payments or shares medical information electronically, a clear line should be drawn between the church and medical entity including not sharing fax machines, computers or files.

2. If church members are healthcare professionals or hospital volunteers, including ministers that volunteer as chaplains, they should never share patient information they learn in that function. If a patient requests to have the church pray for them in the course of conversation with the member, the member should only share that a patient asked for prayer and not share protected health information. The patient's name or other demographic information should not be shared. Pastors and others from the church should not use the relationship with the member to find out information about another member or someone from the community who has been seen in that member's work setting. It sets up the member to break confidence and be subjected to fines.

3. If the church member employed in a hospital sees a fellow member in the hospital, she should ask the other member if he would like the pastor notified. If the member responds in the affirmative, a note should be placed in the medical record to that effect.

4. The regulations allow most healthcare facilities to confirm if someone is a patient in their hospital, but you must have the correct name of the patient. When calling or going to the information desk, make sure you know your members legal name, not a nickname or a maiden name.

5. There are times further protection may be required. If a patient is considered a no news or private patient, then the healthcare facility cannot release information without a code number or other identifying information.

The following are five suggestions that churches might wish to implement to protect their members privacy.

1. Ask before placing someone on the prayer list, there are many reasons people do not want others to know about their illness.

2. Only place the name on the prayer list. Ask the person what information they would like shared when someone inquires.

3. Be very careful about placing names on public web pages, this provides information for those who might wish to do someone harm.

4. Have a clear policy about what your church places on social media sites such as Facebook making sure it is keeping with the wishes of all those involved.

5. If you are not sure about whether to share the information always err on the side of protecting the privacy.