

Confidentiality in Healthcare

By Claudia Brauer

Are you committed to confidentiality?

Can you assure your client that you are protecting their patient's privacy?

Recently someone asked in a forum if they could discuss with a counselor or a spiritual advisor an issue they had been exposed to during a healthcare interpreting session and which was causing them a lot of distress, even after a few days of the event.



Image: ilypasscoordinationproject.org

First of all, keep in mind that any breach of confidentiality is irreversible. Once confidential information or documents are shared, they cannot be unshared, erased or deleted. The same happens with any words you say. Once they come out of your mouth, you cannot un-say them.

Confidentiality of a patient's information means that no one outside the authorized individuals should be able to IDENTIFY the patient from the information you release. That means that whoever you release any of the information you have gained should be absolutely unable to IDENTIFY the patient at any point in time.

Thus, as long as what you share does not IDENTIFY the patient, you would be able to share your experiences with a counselor or a spiritual advisor.

The trick therefore lies in to avoiding disclosure of "where" it was that you obtained the information (i.e., you should not say, I was at an interpreting session in Baptist hospital, for example); who was involved (you cannot say, Dr. Smith was seeing a patient from Nicaragua); and not revealing specifics about the case (the lady had been raped by her brother, who works at the local branch of XYZ bank).

But you could share, for example, that you were in an interpreting session where a doctor was seeing a patient who had been raped by her brother. Since this information does not identify the patient, then you could share it, provided that you have a REASON for sharing it (your mental wellbeing, not just gossip) and that the person you are sharing it with is also a professional code of ethics that would prohibit them from sharing it with third parties (i.e., a mental health or spiritual counselor, for example, who by their own profession are bound by the rules of confidentiality).

You cannot share it with a friend or relative. You cannot discuss it in detail in open forums. You cannot write about it to someone else.

In the United States, HIPAA⁽¹⁾ regulations clearly state the "IDENTIFIERS" of what is called "PROTECTED HEALTH INFORMATION", which are those identifiers that you cannot share with others. They include name, address, telephone, fax, email, social security number, medical record number, account number, health plan number, drivers license number, vehicle identification, device identifiers and serial numbers, names of relatives, URL, IP address, biometric identifiers, photos, date of birth, admission date, discharge date, date of death, exact age, and in general, any other UNIQUE IDENTIFYING NUMBER, CHARACTERISTIC or CODE.

Maintaining the privacy and confidentiality of a client's information, obtained verbally, in writing, or any other way, is very serious business. Pursuant to ISO-17799⁽²⁾: "Confidentiality (implies) ensuring that information is accessible only to those authorized to have access." Additionally, privacy means, "not being available for public viewing or knowledge," and private information should always be treated as confidential information. Finally, Protected Health Information (PHI) is "any information about health status, provision of health care, or payment for health care that can be linked to a specific individual." (HIPAA definition)

 <p><small>Image: nycpartnerforfamilies.org</small></p>	<p>So, in short, you can only share your thoughts or information outside the encounter if and when:</p> <ul style="list-style-type: none">(a) it is with the treatment team authorized to know the information;(b) it is with a professional bound himself/herself by confidentiality;(c) you do it because you "need" to, not because you "want" to (gossip); and(d) you do not reveal any specific information that would allow the individual to be identified.
---	---

Let's suppose you have a secret from your youth and for some reason, you must translate some related documents into French. You trust the translator. However, your secret gets posted on Facebook. How would you feel? The same feeling and the same reaction could be that of your client if some confidential information they provided during an interpreting encounter suddenly became known to others. Not nice, right?

In my opinion, one of the most important standards of practice and ethical commitments in translation and interpreting is trust and confidentiality. In the ideal world, every translator and interpreters would ALWAYS act as if they had signed a detailed confidentiality agreement for every single assignment they undertake, stating that they will abide by the strictest guidelines and principles of ethics, confidentiality, privacy and physical security.

As a translator or interpreter, we handle huge numbers of documents and large amounts of information, much of which contains sensitive content, private and personal data, and confidential information. There is always great risk that such information may leak out, even unintentionally, unless we take proactive steps to prevent that from happening. It is not enough that the leaking would have occurred due to an "error" on our part. There are very few instances where you can allege real "errors" in the disclosure of private or confidential information. Most of them are preventable and you are required to take very specific steps to ensure you are preventing any unintentional (and intentional) leaks of information.

Confidential information does not necessarily have to be recorded in material format. It may also be information acquired verbally (in person, over the phone or by videoconference), or knowledge gained inadvertently (something you see during an encounter, for example).

To ensure privacy and confidentiality of the information that is provided to us or which we become aware of verbally means that you must have in place rules and protections to preserve the privacy of the persons as well as the confidentiality of their information, which, once we know by us, is considered to be under our care. It also means that such information and documents must be kept in strict confidence and that access must be granted or provided solely to those specifically authorized by the owner or by law.

(1) HIPAA (<http://www.hhs.gov/ocr/privacy/>) - "The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information."

(2) ISO-17799 (<http://17799.macassistant.com/def.htm>). ISO17799 is a detailed security standard organized into ten major sections, each covering a different topic or area. These include, amongst others, physical, personal and environmental security measures to prevent unauthorized access, damage, and interference to information; and to prevent compromise, theft or disclosure of information; to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements; to reduce risks of human error, theft, fraud or misuse of information; to ensure that users are aware of information security threats and concerns, and are equipped to support the security policies in the course of their normal work.