



Four Mistakes You Should Avoid



Few U.S. healthcare professionals--or their HIPAA consultants—fully understand the Privacy Rule or the Oral Privacy requirement. They've simply been very busy with other things including other aspects of HIPAA. But when you ask them, they tend to make one or another of the following mistakes about Oral Privacy—all of which are wrong.

Court judges simply don't regard the fact that you may be ignorant of something that is obvious as an acceptable and appropriate defense for someone in a professional capacity.

First, many professionals and consultants assume that Oral Privacy is subjective, that it can't be measured or monitored objectively. They're wrong about this. In fact, Oral Privacy is what lawyers call a "term of art." That is, a precise, measurable, public and professionally accepted definition of it exists that judges and juries can easily identify and understand.

In fact, the scale on which Oral Privacy is measured and the electronic instruments used to measure it have been around for quite a while. So ignorance of this fact is not really a very reasonable defense.

Second, most people—professionals and consultants alike--assume that there aren't any published standards or best practices for Oral Privacy that could provide a useful framework for a HIPAA compliance program. They're wrong. Standards and best practices have been around for several decades. They're the result of the fact that other government agencies like DOD, DARPA and GSA have long been concerned about privacy.

In fact, judges and juries can easily find precise, measurable definitions of three different kinds of "Oral Privacy"—i.e., "Confidential Privacy," "Normal Privacy" and "Minimal Privacy"—simply by using these standards.

Third, many have assumed that there were "loopholes" that meant they could safely ignore the whole thing. But this is both dangerous and wrong. The loophole most have been counting on is the phrase "incidental disclosures." In fact, "incidental disclosures" are only permissible provided "reasonable safeguards" have been put in place to prevent them.

The Privacy Rule says: "an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards...is not a permissible use or disclosure and, therefore, is a violation of the Privacy Rule" (164530[c]).

Fourth, most healthcare professionals and consultants have simply assumed that Oral Privacy can't be fixed without going to the inordinate expense of building walls. This is, of course, impractical in many healthcare situations, such as at nursing stations and in wards and emergency rooms where open communication is essential. They're dead wrong about this. In fact, simple, practical, non-structural—even invisible—"fixes" are available.



What does the term “Reasonable safeguards” mean?

Like “Oral Privacy,” “Reasonable safeguard” is a term that has specific, legal meaning, so you need to be careful. One definition of “reasonable” is simply “ordinary or usual.” But certainly, what judges and juries would expect this to mean is probably more demanding than what the people at DHHS say they intended it to mean.

What DHHS people say is that they expect you and your healthcare organization to put in place solutions that are based on accepted standards. They also expect you to base your approach on “best practices” that have already been tried and proven elsewhere. And they certainly expect you to put in place solutions that can be measured and monitored periodically so you can keep a record to demonstrate that you are in compliance.

They DO NOT expect you to build walls or do anything else that impedes the flow of critical healthcare communication or the provision of medical services. The bottom line is they expect you to be informed and intelligent about the matter. They expect you to have given it sufficient consideration, and to have expended some effort and/or resources to fix the situation in order to “reasonably safeguard” the privacy of oral communication.

Here is exactly what the Privacy Modification Final Rule says. “The Privacy Rule generally requires covered entities to make reasonable efforts to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose (sec. 164.502[b]).”

And it says (sec. 164.530[c]) “the Privacy Rule requires covered entities to implement appropriate administrative, technical and physical safeguards to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that violates the Rule...**including information transmitted orally**, or in written or electronic form.”

And it says “An incidental use or disclosure [is] permissible only to the extent that the covered entity has applied reasonable safeguards as required by sec. 164.530[c].”

And it also stipulates that “an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not a permissible use or disclosure and, therefore, is a violation of the Privacy Rule.”

And it adds that “The Department does not intend with this provision to obviate the need for medical staff to take precautions to avoid being overheard, but rather, will only allow incidental uses and disclosures where appropriate precautions have been taken.”