
WEDI - Strategic National Implementation Process (SNIP)

Oral Communications: Myths and Facts White Paper



SNIP

**Oral Communications: Myths and Facts
White Paper – Version 1.0 – April 2003**

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange

12020 Sunrise Valley DR., Suite 100, Reston, VA. 20191

(t) 703-391-2716 / (f) 703-391-2759

© 2003 Workgroup for Electronic Data Interchange, All Rights Reserved

Contents

Oral Communication: Myths & Facts	1
Disclaimer.....	1
Introduction	1
Why should you care?	2
Four myths & the real facts you should know	2
Myth #1:	2
Myth #2:	2
Myth #3:	3
Myth #4:	3
What does the term “reasonable safeguard” mean?.....	3
A simple “solutions tool kit”	4
What do NRC, STC & HTL mean?	4
What’s the most effective solution?	5
“Oral Privacy”	6
Three levels of “oral privacy”	6
Six oral privacy standards you should know.....	7
Sobering statistics: recent healthcare privacy lawsuits	7
Example A: “Got cancer? Sorry, but we’re calling your loan”	7
Example B: “You’ve got HIV—just kidding!”	8
Example C: “Daddy, the drug store man says you have AIDS”	8
Example D: “Dumped? We’ll help you get even...”	8
Example E: “But judge, I didn’t mean it”	8
Example F: “Arming your Ex”.....	8
Other examples.....	8
Conclusion: first, take some measurements	8
Other Sources of Information	9
Acknowledgements	10

Oral Communication: Myths & Facts

Disclaimer

This document is Copyright © 2003 by The Workgroup for Electronic Data interchange (WEDI). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided "as is" without any express or implied warranty.

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

Introduction

How do we deal with the “oral communications” requirement that Congress put into HIPAA? It is a section that many people do not understand. Many also believe that oral communications are simply a matter of lowering your voice. Most people do not really know how to fix the oral communications environment.

Amazingly, this is easy to fix. And no, you don’t need to build walls to achieve compliance, and it does not cost much either. The irony is that the “oral communications” requirement is absolutely straightforward. There are simple technology fixes can be learned from other industries. Standards were developed decades ago to measure and monitor oral communications – at the urging of federal

government agencies like the Department of Defense (DoD), the United States Defense Advanced Research Projects Agency (DARPA), and the General Services Administration (GSA). Most of the “fixes” have long since been turned into suitable, rated products you can buy off-the-shelf at home supply stores – even from websites – without leaving your chair. The background on oral communications that is in this white paper provides you with the information you need to meet the oral communication requirements of HIPAA.

Why should you care?

Many people think that the oral communications mandates within the Privacy Rule do not really matter. Although the Final Rules were not issued until 2001, the fact is that State courts around the U.S. have been using HIPAA law and regulations as the “standard of care” since Congress passed it in 1996.

In fact, there are already a number of cases with substantial damages awarded as the result of healthcare privacy violations (see www.healthprivacy.org for a summary of sixty such suits). The largest of these suits was for \$14 million against a research hospital. This paper outlines six “Recent Privacy Lawsuits” below.

Four myths & the real facts you should know

Few healthcare professionals are yet fully informed about the oral communications requirement. They’ve simply been very busy with other things including the many other aspects of HIPAA. When you ask them, they tend to make one or another of the following mistakes about oral communications – all of which are wrong. Below are four common myths and the facts about these myths.

Myth #1:

Most professionals and consultants assume that oral communication is entirely subjective, that it cannot be measured or monitored objectively. This is a myth. A precise, measurable, public and professionally accepted definition of oral privacy, or “speech privacy” exists that all, including judges and juries, can easily identify and understand. There are six standards that apply here. They’re interrelated, and they’re published by ISO, ANSI and ASTM – all recognized standard setting organizations. The oldest of these standards has been in active use since 1969 in numerous federal government agencies as well as in industries like defense, banking, insurance, manufacturing and publishing. In other words, the standards provide you with a set of convenient and proven “best practices” for addressing HIPAA’s oral communications requirement.

The scale or index on which oral communication can be measured and the electronic instruments used to measure it have been around for over 30 years.

Myth #2:

Most people assume that there are not any published standards or best practices for oral communications or “speech privacy” that could provide a useful framework for a HIPAA compliance program. This is a myth. “Speech privacy” standards and best practices have been around for several decades. They are the result of other government agencies like DoD, DARPA and GSA having long been concerned about privacy. Industries like banking, insurance, manufacturing and publishing have also been concerned about “speech privacy”.

Myth #3:

Many people assumed until August 14, 2002 when the Privacy Modification Final Rule was published, that oral communications could safely be ignored or at least considered a low priority. This is a myth. The term most have been counting on is “incidental disclosures.” In fact, “incidental disclosures” are only permissible provided “reasonable safeguards” have been put in place to prevent misuse or inappropriate disclosure of protected health information.

The Privacy Final Rule state: “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]). But what are “reasonable safeguards”? Reasonable safeguards are discussed below.

Myth #4:

Most people have assumed that Oral Privacy or “speech privacy” can’t be fixed without going to the inordinate expense of building walls. This is a myth and, of course, impractical in many healthcare situations, such as at nursing stations and on floors and emergency rooms where open communication is essential.

In fact, simple, practical, non-structural – even invisible – “fixes” are available. In many cases they’re off-the-shelf and can be bought at home supply stores and over the Internet.

What does the term “reasonable safeguard” mean?

Like “oral communications,” “reasonable safeguard” is a term that has specific meaning. 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 DHHS may have intended.

What DHHS has said 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. 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.

DHHS DOES NOT expect you to build walls or do anything else that impedes the flow of critical healthcare communication or the provision of medical services. You need to be informed and intelligent about the matter. Consideration and expenditure of some effort and/or resources to augment what you already have in place will go a long way to being a “reasonable safeguard” of oral communications or “speech privacy”.

The Privacy Modification Final Rule states:

“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” (45 CFR 164.502[b]).

“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.”

“An incidental use or disclosure [is] permissible only to the extent that the covered entity has applied reasonable safeguards as required by 45 CFR 164.530[c].”

“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.”

“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.”

A simple “solutions tool kit”

A good HIPAA Oral Privacy “tool kit” will only have four things in it. Most of these things are available off-the-shelf or from the phone book or from web sites. In addition, you can use them separately or in combination to achieve the level of privacy you need or want to achieve. Here is your tool kit:

1. NRC and STC-rated ceiling tiles (they absorb sound so that conversations don’t “travel”).
2. “High TL-rated curtains” (they block sound so that the person in the next bed can’t understand the conversation you’re having with your doctor)
3. NRC and STC-rated portable panels (they absorb and block sound)
4. “White noise systems” (also known as “speech privacy systems, ”) that have been tested to meet the technical standards for “speech privacy”.

What do NRC, STC & HTL mean?

The technical terms like “NRC,” and “STC,” are accepted, standards-based acoustical terms and are well understood at home goods stores. You can always ask a salesperson there: “what’s the NRC or STC rating of this ceiling tile?” You can expect to get a very explicit answer. Sometimes it’s even listed right on the product. If not you may look it up on the supplier’s website.

In fact, all of these terms are widely and conventionally used in the building products and office furniture industries – and have been for decades. They owe their existence to the same U.S. government agencies that, decades ago, urged the development of the standards – DoD, DARPA and GSA. Here is what these terms mean:

- NRC is “Noise Reduction Coefficient.” It’s a standardized measure of the extent a ceiling tile or a curtain or a portable panel actually absorbs sound waves, preventing the waves from bouncing around and “traveling” to where other people can hear them.
- STC is “Sound Transmission Coefficient.” This is a standardized measurement of the material actually blocking sound waves. For example, most “office cubicles” are made of “soft” panels

that are covered by fabric behind which is some padding backed by a stiff board all of which give the panel higher NRC and STC ratings.

- High TL means “High Transmission Loss.” This too is a way of describing the relative ability of a material to prevent sound waves from traveling directly through it.
- “Speech privacy system or white noise system”(also known as “sound masking”) is a technology that was developed in the late 1960’s to meet the needs of security-conscious government agencies for confidentiality and speech privacy.

Remember the phrase: “loose lips sink ships”? That’s where the impetus for standards development came from. Acoustical privacy products and technology have gone through several generations of development since the 1960’s. Currently, they are installed in about one hundred million square feet of new corporate and government office space in the USA every year at companies like Aetna-US Healthcare, IBM, Verizon, AOL, and Fidelity. So chances are you’ve been in a space with “speech privacy” or “sound masking” technology before and didn’t even know it.

What’s the most effective solution?

Of the four things in your HIPAA Tool Kit, “speech privacy (or sound masking)” is the one that can have the greatest impact. The latest digital technology has brought the cost of speech privacy systems down so that you can now “treat” an area as small as an elevator or a psychiatrist’s waiting room for approximately \$150.

The technologies behind “speech privacy (or sound masking)” came out of work by scientists and engineers in the 1960’s establishing that “speech privacy” is a matter of making speech “unintelligible.” That is, if each of us can’t understand what the other is saying, we effectively have established “speech privacy,” even though we may still be able to see and, to some extent, hear each other. In fact, the first documented application of “speech privacy technology,” back in 1964, was in a healthcare facility.

What a “speech privacy system” ” does is to “fill in” the sound spectrum around you with barely perceptible “white noise” so that speech is rendered unintelligible. It’s actually designed to sound like typical office air conditioning noise so that you won’t notice it. In other words, it is often described as a “gentle wooshing sound.” This does not impede an elevated conversation from a nursing station to a doctor passing in the hallway. The individual in the hallway would hear his or her name called even with a “speech privacy” system turned on.

Walls are not necessarily needed to achieve oral privacy or speech privacy using a “speech privacy system.” And this makes it an excellent solution for most healthcare situations, everything from emergency rooms to nurses’ stations to waiting rooms all the way to the call centers at health insurance companies where customer service people handle patient inquiries.

If you want to look into this particular solution, you will find numerous sources for “speech privacy (or sound masking)” by typing the key words “HIPAA sound masking” or HIPAA white noise” into a search engine. But be aware that there are a variety of different approaches to this technology and that cost and quality can vary dramatically depending on the technology and installation methods used. In fact, cost may range from as low as \$0.45 per square foot with only a few isolated areas needing to be covered (this is called “zoning”) to as high as \$6 or \$7 per square foot with the caveat that that entire floors of a building must be covered because the electronics must be driven from a central equipment closet.

The two basic types of “speech privacy (or sound masking) technologies are:

1. “Reverberant field” or “plenum” systems: these are the oldest and most expensive to purchase and install and have been in use since the 1960’s.
2. “Direct field” systems: these are the newest, lowest in cost, easiest to install systems and have been in wide use since about 1998.

When inquiring, be sure to call several sources, to ask about the type of technology used, to inquire about the complete installed cost, and to ask about whether the source has a thorough understanding of HIPAA’s oral communications requirement and the applicable published standards, what it means to comply with them, and how they will measure and certify performance.

Prices can range from \$150 to hundreds of thousands of dollars depending on the type of technology used, how long it has been in use and how a particular supplier goes about installing it. You should also ask about the supplier’s experience meeting the HIPAA requirement to know whether a supplier already understands HIPAA compliance. You also need to know whether a particular supplier knows how to take the necessary measurements to determine whether the solution they propose will actually make your facility HIPAA compliant or not.

“Oral Privacy”

A suite of six standards (see below) from three widely accepted standards organizations – ISO, ASTM and ANSI – give precise definition to the term “oral privacy” or “speech privacy”. They are objective and accepted. These standards have been widely practiced and publicly available for decades. The first of them was originally published in 1969 and has been in continuous and active use since then. So they effectively form a set of “best practices.”

They were developed over four decades to meet the needs of corporations, institutions and government agencies like DoD, DARPA, GSA and NIH. All of these agencies have been concerned with the problem of preserving confidentiality and privacy in work environments that have become increasingly “open,” i.e., without walls. This mirrors circumstances found in most healthcare organizations where privacy must now be protected.

These standards explain the physics involved and lay out a proven measurement scale – something called the “Articulation Index” which has been described in acoustics textbooks since the 1950’s. In addition, the standards give precise numbers for each of three different levels of “oral privacy” or “speech privacy.” This means you can choose the level of compliance you want to achieve in your organization and then budget accordingly.

Instruments are also available from several sources for taking the appropriate measurements. They are no larger than a laptop computer and some operate on batteries. Some training is involved in using them.

Three levels of “oral privacy”

Here is how one of these standards, ASTM E1130.02.e1, precisely and straightforwardly defines the three different levels of “oral privacy.” After you’ve read this section, ask the following four questions: (a) Which of these suits your needs? (b) Which of these would be the most likely choice of your board of directors and of your organization’s legal counsel? (c) Which of these best fits the reality of your organization’s budget? (d) Which of these can be practically accomplished?

1. “Confidential privacy” – “Speech privacy described as ‘confidential when speech cannot be understood. This degree of speech privacy is indicated at Articulation Index values at or below 0.05.’”
2. “Normal privacy” – “At Articulation Index values between 0.05 and 0.20, ‘normal’ speech privacy is indicated. In this range concentrated effort is required to understand intruding speech.”
3. “Unacceptable privacy” – “Speech becomes more readily understood at Articulation Index values greater than 0.20. Some describe ‘unacceptable’ privacy as values above 0.30. At Articulation Index values above 0.40, there is essentially no privacy.”

Six oral privacy standards you should know

- | | |
|---------------------|---|
| 1. ASTM E1130.02.e1 | Standard test method for objective measurement of speech privacy in open offices using Articulation Index (AI) |
| 2. ASTM E1110-01 | Standard classification for determination of Articulation Class |
| 3. ANSI S3.2 | Method of measurement of monosyllabic word intelligibility |
| 4. ANSI S3.5 | Methods for the calculation of Articulation Index (AI) |
| 5. ISO 60258-16 | Objective rating of speech intelligibility by Speech Transmission Index (STI) |
| 6. ISO 9921-1 | Speech interference level and communication distances for persons with normal hearing capacity in direct communication (SIL method) |

Sobering statistics: recent healthcare privacy lawsuits

Judges and juries in State courts around the U.S. have been hearing healthcare privacy lawsuits for a number of years and are now beginning to use HIPAA as the “standard of care.” The damages and fines awarded to plaintiffs in these cases are significant. There is also a significant loss of reputation in some suits.

Here’s a look at several cases that illuminate the issues underlying healthcare privacy and the financial cost that can result for healthcare organizations that have not complied with the law. You can find summaries of sixty such lawsuits at the website www.healthprivacy.org. Notice that several of these cases involve some “oral communication.”

Example A: “Got cancer? Sorry, but we’re calling your loan”

A banker who also served on his county’s health board cross-referenced customer accounts with patient information. Then *he called due* the mortgages of anyone suffering from cancer (The National Law Journal, May 30, 1994, p. A1).

Example B: “You’ve got HIV—just kidding!”

The 13-year-old daughter of a hospital employee took a list of patients’ names and phone numbers from the hospital when visiting her mother at work. As a joke, *she contacted* patients and told them they were diagnosed with HIV (The Washington Post, March 1, 1995).

Example C: “Daddy, the drug store man says you have AIDS”

A man with AIDS won an out-of-court settlement with a Michigan pharmacy in 1998. A pharmacy clerk *told the man’s children* that he had AIDS (Chicago Tribune, January 9, 1998, p. 10).

Example D: “Dumped? We’ll help you get even...”

A former patient of Johns Hopkins Hospital sued for \$12 million alleging that the hospital released his medical records to a former friend and business partner who subsequently *gave information* about his drug abuse problems to friends, family, business associates and clients (Baltimore Business Journal, January 14, 2002).

Example E: “But judge, I didn’t mean it”

A Wisconsin jury found that an EMT invaded the privacy of an overdose patient when *she told* the patient’s co-worker about the overdose. The *co-worker then told* nurses at the hospital where both she and the overdose patient were also nurses. The EMT claimed *she called* the co-worker out of concern for the patient. But the jury found that regardless of her intentions the EMT had no right to disclose confidential and sensitive information and directed the EMT and her employer to pay a fine for the invasion of privacy (Milwaukee Journal Sentinel, May 9, 2002).

Example F: “Arming your Ex”

Longs Drugs in California settled a lawsuit filed by an HIV positive man. After a pharmacist inappropriately *disclosed* the man’s condition to his ex-wife, the woman was able to use that information in a custody dispute (San Diego Union-Tribune, September 10, 1998, p. A3).

Other examples

Other high-profile privacy cases you might want to look at on this website are those involving country music star Tammy Wynette, Congresswoman Nydia Velasquez and tennis star Arthur Ashe. But as the stories above show, healthcare privacy affects more than just the rich or the famous.

Conclusion: first, take some measurements

To get somewhere, it helps to know where you’re starting from. Obviously that’s why most healthcare organizations begin their HIPAA compliance programs with a “GAP Analysis”. This sets the compliance benchmark. To get started on oral privacy compliance, you need to get some basic measurements done of your facility and add these and some budget estimates to your organization’s “GAP Analysis.”

You or someone on your team can quickly and easily identify capable professional resources by using a search engine with key words like “HIPAA oral privacy” or “HIPAA sound masking” or just “white noise” or “sound masking.” Alternatively, you might check your Yellow Pages under “acoustics engineering.”

We recommend you conduct a telephone interview with several of these sources to ensure that they are thoroughly familiar with the Final Privacy Rule, that they understand your HIPAA compliance needs, and that they have the tools and the skills needed to help you. Be sure to tell them that you want a written, fully documented report to include in your GAP Analysis. You want this report to contain a complete set of privacy enhancement recommendations to include in your organization’s budget planning.

The consultant should be able to show you an example of this kind of report from another healthcare facility that they have surveyed. In any case, taking a set of acoustic measurements of a healthcare facility doesn’t take much professional time, so it should not be a large expense.

For example, a one hundred-sixty bed hospital is likely to have about twenty different “typical” sites that need to be measured including emergency rooms, post-operative recovery rooms, waiting and reception areas, nurses stations, pharmacy counters, consultation rooms and screening areas. A capable consultant can take a quick walk through your facility and identify the “hot spots” you should measure. Alternatively, you can identify these yourself and simply ask for an estimate of cost based on the information you provide.

Acronyms

- ANSI is the American National Standards Institute
- ASTM is the American Society of Testing and Materials
- DoD is the U.S. Department of Defense
- DARPA is the U.S. Defense Advanced Research Projects Agency
- GSA is the U.S. General Services Administration.
- ISO is the International Standards Organization

ISO, ASTM, and ANSI are widely respected as the publishers and repositories of an abundance of technical standards covering many technologies and industries.

Other Sources of Information

WEDI/SNIP Web Site

snip.wedi.org

Workgroup for Electronic Data Interchange (WEDI)

www.wedi.org

OTHER SOURCE: Specific information on the applicable standards for Oral Privacy from ISO, ANSI and ASTM are posted at CSM/Acentech’s (formerly BBN Acoustics) website: www.acentech.com/ssHIPAA.htm. Copies of the full text of these standards may be ordered from the standards agencies.

Acknowledgements

WEDI/SNIP would like to express its appreciation to the authors for their efforts in preparing this White Paper:

David M. Sykes PhD
Vice President, CSM/Acentech (formerly BBN Acoustics), and
Managing Director, The Remington Group LP, Cambridge, MA.

Susan A. Miller, Esquire
The Kearney Group
HIPAA Certified LLC