

HIPAA Compliance Made Easy: Dispelling HIPAA Myths,
with John Murdoch

Narrator: Good Morning. Welcome to Wilentz Goldman & Spitzer's web t.v. broadcast. My name is Michael Schaff. I'm a shareholder at Wilentz Goldman & Spitzer. It's Your Legal Rights program and tonight, or this morning we're going to be talking about is HIPAA compliance made easy, dispelling HIPAA Myths. We're going to have with us this morning a speaker, John Murdoch. John is an associate of the Wilentz Goldman & Spitzer law firm, where he is an expert in HIPAA compliance matters. John focuses his practice on complex regulatory issues and business transactions involving health care professionals. John has assisted many physicians, chiropractors, physical therapists and licensed health care facilities, in compliance with the myriad of HIPAA regulations and has presented many seminars on HIPAA compliance matters to health care professionals and attorneys. In addition to the many seminars that John has done on HIPAA compliance, John recently authored the HIPAA Security Regulations, What Physician Practice Should be Doing Now and he was also recently named by the New Jersey Department of Banking Insurance to the Department's HIPAA implementation task force. John is an active member of the American Health Lawyers Association, the American Bar Association, and the New Jersey State Bar Association's Health and Hospital Loss section, where he is a director and currently serves as the secretary of the section. Prior to joining Wilentz Goldman & Spitzer in the year 2000, John served as special assistant to the Commissioner of Banking and Insurance in New Jersey.

During this broadcast, you'll have the ability to ask questions by submitting a question by the instant message interface on your screen. Before we start, however, I'd like to have a few words of caution. This session is really for general information purposes and should not be deemed legal advice. In order to get specific legal advice, you should directly consult with an attorney. With that I'll turn it over to John.

JM: Good morning, Michael.

MS: Good morning.

JM: Well thank you very much for having me here today.

MS: Thanks. John, there's been a lot of things with respect to HIPAA out there and scaring health care practitioners. What is a business associate that uses that word constantly? Do you know what that is? Can you explain that to our audience.

JM: Yeah, it's a, a business associate is a person or an entity that performs a function on behalf of a covered entity, and I'm going to go into what a covered entity is in a moment. But a business associate basically performing the service on behalf of the covered entity has access to patient health information. And by having that access to patient health information they need to make sure that, the covered

entity needs to make sure that that business associate is protecting that patient health information so it's not improperly disclosed or leaked out.

I guess, just stepping back, I was so appreciative to have this opportunity to come here to speak about these issues today, because there's so much misconception, so many misunderstandings out in the health care community regarding HIPAA. A lot of it began when the HIPAA privacy regulations first were adopted. The regulations were so strict in the reading that people were screaming, how are we possibly going to protect this patient health information? We can't even do things like calling patients names in a waiting room. We can't have sign-in sheets. There were so many potential restrictions, so much fear among health care providers. That was kind of clarified in August of 2002 and we'll talk about that as we go on.

But for anybody who's watching here today, really, the HIPAA privacy regulations, which we're focusing in on today, apply to what's called covered entities. And covered entities are either health care providers who conduct a covered electronic transaction, health care clearing houses, and they're the entities that take claim information, convert it from non-standard to standard, and then vice-versa, when the health care claims are submitted to payers and the information is transmitted back to the doctor's office. Also, health plans. So these are the three categories that are covered under HIPAA. So, as a health care provider who conducts one of the covered electronic transactions, you're now brought within complying with the HIPAA privacy regulations, and you have to take a lot of steps to make sure you comply with the information. And generally those steps are having written policies and procedures on how to comply with HIPAA, designation of a privacy official to be the person who is responsible for the practices, compliance with the privacy regulations. Also, have training for your work force. You also have to have a process to receive complaints from patients regarding use and disclosure of their information. You have to have a notice of privacy practices, and I'm sure you've probably seen that. Everybody's seen that when they've gone into the pharmacies, their doctor, their chiropractor's office, hospital. Several page document saying how that health care provider is going to use and disclose their health information. So those are the general issues.

And now getting back to business associate, you have situations where a person who is not a covered entity is not required to comply with HIPAA. For example, us as attorneys. When we perform work on behalf of a physician, then it follows use of disclosure of patient health information. And a great example that comes up all the time is disputes with _____ payers. And we have Mary Smith's name --

MS: -- by payers you mean insurance --

JM: -- Insurance companies. So if we have Dr. Smith comes to us and says, "I have a problem with this claim, it's not being paid by insurance company 'x'", and he discloses that patient's information to us, we are now performing a function of

behalf of that covered entity. We're not covered under HIPAA so we don't have to comply pursuant to HIPAA, but because we're now a business associate of that health care provider we have to have an agreement with that health care provider saying that we're going to protect that health information.

MS: Now what kind of health care information are we talking about here?

JM: Oh, it's a good question. It's any information that pertains to a patient. So, now, there's some subtle differences, there's some subtle exceptions within the HIPAA privacy regulations, but I caution all health care providers that whatever they have pertaining to a patient, name, address, telephone number, health condition, etc., is all protected health information. They need to make sure they comply with the HIPAA privacy requirements by protecting all that information. And not to get caught up in some of those subtle exceptions. And I wouldn't even worry about those. Just protect everything you have.

MS: Okay. Now, what does a health care provider need to do with their business search? You, we already mentioned where a business _____. What would you need to do? You believe someone is a business associate, what do you need to do now as a health care provider?

JM: Now, as a health care provider, again, as we discussed, you're covered under HIPAA, you have to comply with the requirements and the HIPAA privacy requirements require you to have what's called a business associate agreement. That business associate agreement basically, it's kind of an ingenious was that health and human services extends the requirements of the HIPAA privacy regulations to these entities that are not covered under HIPAA. So, the covered entity, in this example the physician, would have a business associate agreement with us as their attorneys, and we would agree not to use or disclose that patient health information other than as required for the purposes we're performing.

MS: What about a transcription service that they use, they deal with? Would they need a business associate --

JM: Yes.

MS: agreement? Yes.

JM: So any person or entity that's performing a service or function on behalf of that covered entity that involves the use of disclosure, protected patient health information. It's amazing. I've worked with probably 40 or 50 different physicians, chiropractors, licensed health care facilities in coming into compliance with the HIPAA privacy regulations and the question comes up all the time, well what about janitorial services? And we had a unique situation --

MS: -- what about janitorial services?

JM: In that case, you have someone, let's say who's coming into your office as, they're performing services – they actually are close to the patient records but as part of their job they're not supposed to have access to those records. So, technically, they're not a business associate and therefore you don't have to have a business associate agreement with them. We get an issue where one office had insisted that the supplier of towels sign a business associate agreement and the towel supplier refused to, saying I wasn't a business associate. And again, even having a person or entity on site, if they're not supposed to access patient health information, they're not a business associate.

MS: I've gotten a lot of questions on a bunch of different issues, and the standard types of questions that we see are things like, "I was told that if I have less than 10 members on my staff I don't have to comply with HIPAA." Is that true?

JM: No, and I'll tell you, this is one of those myths that I really wanted to talk about today. And this myth was so prevalent that it appeared in some newspapers. There was a newspaper in Texas that actually printed this misinformation. Some of the HIPAA experts, nationally, were passing along this information, which made it very confusing.

MS: I guess they really weren't experts.

JM: No, I guess not. And it made it difficult because a lot of these so-called experts were gathering little bits and pieces from different pieces of legislation and regulations and they thought that if you had 10 or less full-time employees that you weren't covered by HIPAA, but that's not true. What that actually pertained to was that as of October 16, 2003, health care providers, physicians who had ten or more full-time equivalent employees had to submit their initial claims to Medicare electronically. Now, by doing so now you're automatically a covered entity but if you have ten or less full-time equivalent employees you are not required to submit claims initially to Medicare. And that's what _____. So, in this case, if you are a solo practitioner and you conduct one of the covered electronic transactions, and what those transactions are, submitting, typically, bills to an insurance company for payment, referrals, electronic, the coordination of benefits. Anything, if you're doing anything electronically, most likely you're going to be a covered entity.

MS: By electronically you mean via the e-mail, or over the telephone, or?

JM: Oh, great question. Basically, electronically would be through a computer system. So, if you're calling up on the phone that's not going to be covered for electronic transaction.

MS: But today most practices submit electronically because they want to get paid, so almost all practices will be deemed submitting it electronically and therefore applicable.

JM: That's --

MS: So that means whether you're a solo practitioner with two employees or one employee or whether you're a large practice with 100 employees, you're still going to be responsible for the compliance.

JM: That's right. And you know a question that's come up many times is that, I'm a small provider, I only have two employees, and I want to submit electronic claims for insurance company "x", but that's it, I don't want to submit electronic claims to any other payer. Am I covered? Yes you are. As soon as you submit that one electronic claim or one of the other covered electronic transactions, automatically you are now a covered entity and you have to comply with all of the HIPAA privacy regulations.

MS: Okay. One other question that I get a lot is, everyone is so confused about the HIPAA regulations and there appears to be many different dates that seem to come across and when things are compliant, when you have to deal with things. What dates should a practice be concerned about? Have they all passed? Are there some in the future that they have to be concerned about?

JM: I'll tell you, this is one of the issues that has really caused a lot of confusion among health care providers. And I guess just stepping back, HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It was federal legislation. It was huge. Pages upon pages of different issues pertaining to funding for health care fraud enforcement on the federal level, insuring that persons who went from one employer to another continued to have health care coverage. So, there was many things that were covered by HIPAA. What we're really kind of focusing in on here today are issues that came out pertaining to patient health information. And where these confusing dates come from is that the first set of dates that came up pertaining to patient health information was October 16 of 2002, and that was the date where providers that were submitting claims electronically or conducting one of the covered transactions had to comply. Now, most providers were allowed to take a one year extension as forms they filed for that. That was the October 16, 2003 deadline. But now, April 14 of 2003 was the deadline for the privacy regulations, and as of April 14, 2003, all covered entities, except for small health claims, which we won't address today, for all doctors, hospitals, pharmacies who were covered entities had to comply by April 14 of last year.

Now, the next deadline that's coming up is April 20 of 2005 and that's the subject of the article that you mentioned that I recently authored, and that's the HIPAA security regulations. It's basically the HIPAA privacy regulations going to the next step, and adding more protections for patient health information that's maintained or transmitted electronically. And one thing I urge in the article is that providers not wait until April 1 of next year, they need to start working on it now because there's a lot of things they need to do in reviewing how their practice operates, what information they're using on the computer in transmitting it, and really take a close look and take the time to implement the regulations

appropriately. But that's where all the different dates come up and that's where there's been a lot of confusion on when providers have to comply.

MS: Okay. Will you post that article on a web site or if people want it they can e-mail you and you will provide it to them?

JM: Sure. Yeah. Anybody who would like a copy, more than happy to send it out and they could just e-mail me and I could send that right out to them.

MS: Okay, thank you. One thing that I have a few clients that are either plastic surgeons or cosmetic surgeons, okay? And they don't deal with Medicare, lucky them. And they say they don't submit anything – everyone is paid in cash. Do they still need to comply with HIPAA?

JM: No. And that goes back to what we were talking about before. As a health care provider in order to be covered under HIPAA and the privacy regulations, you have to conduct one of those covered electronic transactions, and we have quite a few plastic surgeons who are exactly in that situation in which everything is paid by cash by the patients. They're not submitting any claims to health insurers and if they are, nothing is being submitted electronically. They're not doing anything electronically. And just an important note when I say they're not doing anything electronically. If they have a billing company that they send the paper claims to and that billing company submits the claims electronically on behalf of that physician, the physician is still a covered entity. They're still conducting the billing electronically. But in a case where the physician practice does everything on paper, doesn't conduct any of the covered electronic transactions, they're not a covered entity, and a lot of people are amazed when they hear that, that they don't need to comply with HIPAA. However --

MS: There's always that however, right?

JM: That's right. I always caution the providers to take a close look at several issues. One, HIPAA is now deemed to be the national standard on protecting patient health information. So here's my concern. Let's say a plastic surgeon said, great, I'm not conducting any of the covered electronic transactions, I'm not a covered entity, I'm just not going to worry about all these requirements. But now let's say patient health information is improperly disclosed and could have been protected if they complied with HIPAA. Now the patient can come back and say, listen, Dr. Smith, my information was disclosed, I was harmed because of this, and you have violated the national standards, the national minimum.

MS: _____ liability.

JM: Exactly. And I caution physicians to take a close look and really evaluate that carefully before they make a final decision.

MS: Okay. Thank you. I have a bunch of questions that have been raised to me that I think may give some examples to the people here who are watching this and

listening, and you know maybe the answers will do it. I had a client who said I have an open reception area, okay? There was no glass divider between the receptionist and the patient waiting room. They asked me, do you need to put up a window or a wall between them? Are you required to make major reconstruction.

JM: You know, it's interesting because part of the compliance efforts that I've done on behalf of health care providers, part of the compliance efforts are actually on-site, taking a look at the physical location of the practice. And quite a few practices are exactly in this situation where they have the open reception area and a lot of the practices feel it's just a lot more friendlier, it's, it just creates a warmer environment for the office. And to answer the question, there's no requirement under HIPAA to make any kind of major renovations, to make any structural changes. You don't have to do that. However, now we come back however.

MS: However again!

JM: What the practice needs to do is to always have throughout the practice what's called reasonable and appropriate administrative, technical and physical safeguards. And what that means generally is they have to make sure that they're doing their best to comply and keep the patient health information protected. And here's where this comes into play in this situation. If you have an open reception area, and usually the reception areas I've seen, they have one or two office staff members sitting behind the receptionist, and they're working on payment issues for patients. You cannot have that office staff member on the phone within earshot of the waiting area saying, oh, I'm calling about Mr. Smith's claim for HIV testing. Of course, that's a violation of HIPAA.

MS: Have some discretion there.

JM: Exactly. So, now what I've devised is that, if you're going to have that open reception area, just make sure that there are no discussions behind the reception area that disclose any patients and their health information, and that any type of activity regarding patient health information is conducted in a separate area.

MS: Is that where the training becomes very important, how you train your staff in what to do?

JM: Yes. And it is something that, again, we talked about April 14 of 2003 being the compliance dates, so all covered entities, all these physician offices, these chiropractors, etc., should have --

MS: Established in place already.

JM: Exactly, well over a year.

MS: Okay, so if they do not have it in place they have to be very careful and they'd better get it in place real soon.

JM: That's right, and I'll tell you, the concern is that you may have situations where the physician, the chiropractor, the physical therapist are very much aware of the HIPAA privacy requirements. Where you're going to blow it is going to be the weakest link in the chain, and it could be that receptionist disclosing some information improperly. And it becomes a concern, especially within physician offices, where everybody knows everybody, and you know, you're in a small town. There's politicians who are treated in that office --

MS: Right.

JM: -- and you know, you can't have someone behind the desk freely discussing that patient's health information within earshot of someone in the waiting room.

MS: Would you recommend that either a consultant or a lawyer come through? Someone who knows something about HIPAA and see how the practice operates and how things run and just have someone do a tour and pick out all the issues associated with HIPAA that may or may not be in compliance?

JM: Yes, I think that's critical. And I think it's important because you need to have someone who is objective. Someone who is not a part of the office staff, because every time I've walked in and pointed out very simple concerns that I had regarding the way the office staff was conducting their business that could potentially improperly disclose information, a lot of times they would be amazed because they'd lived with it so long they didn't notice it.

MS: It may be they don't even notice the obvious.

JM: And one great example is I was asking in one office -- it was an older building, they'd been there for over 20 years -- where are your patient records? And they brought me over to a file cabinet that was locked. I said, there's got to be more. Nobody knew. They called the office manager who was out that day, who said, well, they're in the one patient treatment room. It was a room that patients would come in, would sit there on their own, and it was an unlocked cabinet. But other people didn't even realize that this filing cabinet existed because they had walked past it for so many years and they didn't even realize it and it was for the older treatment records.

MS: _____ goes to another issue. What happens if you, if you have, you're into the technology and you have computers in each room and in fact in a patient treating room and you're able to log right in and dial in, is that a potential violation? Can you leave patient unattended in rooms like that?

JM: Yeah. That's a huge concern. Right now, and as I pointed out before, you have to have the reasonable and appropriate administrative, technical and physical safeguards. And that varies --

MS: Can you say that five times fast?

