Annals of Health Law

Volume 16
Issue 2 *Summer 2007*

Article 10

2007

Transcribed Speech of Stephen Weiser

Stephen Weiser
Health Care Service Corporation

Transcribed Speech of Stephen Weiser

MR. WEISER: Well, thank you, Larry, for your introduction. It was about three years ago that I took on the role of Assistant General Counsel at Health Care Service Corporation. After providing legal counsel to the hospital and healthcare provider industry for over thirty years, I was offered the opportunity to work with one of the nation's top health insurance companies. It afforded me the opportunity to make use of my regulatory background in an entirely different setting. Health Care Service Corporation is a nonprofit Illinois mutual legal reserve corporation operating Blue Cross Blue Shield plans in Illinois, Texas, New Mexico, and Oklahoma. I am proud to say that this year, Health Care Service Corporation was awarded the Best Practices award in regulatory oversight by the Health Ethics Trust at the Healthcare Best Compliance Practices Forum. The Forum awards this prize annually and is the only national organization in which healthcare leaders, top government officials, compliance professionals, and selected legal and academic experts meet in a vendor-free environment to address practical compliance considerations. Health Care Service Corporation is serious about the privacy of its members' healthcare information as well as compliance with a vast array of federal and state laws that regulate the healthcare industry. I am pleased that my colleagues, Nadine Zabierek, who's Vice President of the regulatory office and the Director of the privacy office, and Deborah Hayes, are here today. Thank you for your support.

Today, my focus will be on state and federal laws that provide challenges to the healthcare industry in the administration of the privacy laws that many of us now fondly or not fondly refer to as HIPAA. I am glad that Dr. Kizer preceded me because I think it's going to help me give greater context to some of the points that I'm going to try to make today. What I'm going to try to do is briefly go over the basics. I really know that most of you do not need any highly intensive instruction on HIPAA at this point. [T]hen I'm going to focus on the collection and treatment by health plans [and] health insurance companies of member data in light of the Illinois Insurance Code and when there is more stringent state law, and I'm also going to cover some issues relating to marketing.

Now, while I'm covering Illinois law, just think, in fifty states there are different laws that cover privacy concerns. [T]hink how difficult it is to run

an organization on an enterprise-wide basis when state law, in the realm of privacy, as well as every other area, is different. HIPAA provided us lawyers and compliance officers great challenges in how to figure out how we can meet the needs of all of our members [with respect to] healthcare privacy concerns as one organization. It's very difficult to do.

I am also going to focus on when health plans seek data from providers and I'm going to do it mostly in the context of pay-for-performance, one of the secondary uses that Dr. Kizer mentioned. Now, health insurance companies, health plans, and company entities, we don't need authorization or consent to disclose or use protected health information for payment activities, which includes utilization review and healthcare operations. We specifically stress that we are not healthcare providers, even in the HMO context, but we do engage in healthcare operations, which includes some of those secondary uses of protected health information—quality assessment and improvement activities where we look at patient outcomes, where we develop clinical guidelines and we conduct population-based activities related to improving health care.

In Illinois and under HIPAA, health plans are recommended to disclose, without authorization, protected health information in certain situations. Of course we all know [that] we don't disclose our information to our business associates. When we get a court order, we are required to disclose protected health information for research and other activities. Also, under HIPAA, [certain types of] research is permitted without authorization, but it has to fall within certain safety parameters. There's got to be an institutional review board or a privacy board reviewing the types of investigations that you're doing.

We also had to do research on decedent health information without authorization. HIPAA has also created something called "limited data sets," [which is] partially de-identified information where we can share data with other health plans or other healthcare providers for research purposes. HIPAA, and also [the Standards for Privacy of Individually Identifiable Health Information], provided a statutory framework [and created] individual rights to access information; disclosure accounting, which covers when a health plan or healthcare provider has inappropriately used or disclosed health information; a way to amend healthcare data; a way to ask for confidential communication in the transmission of healthcare data; and the notice of privacy practices that we don't read.

Today, we'll focus on state law, which is more stringent in regard to individual rights, authorizations, disclosure accounting, and marketing. Health plans in Illinois are subject to the Illinois Insurance Information and Privacy Protection Act. Many of you in the healthcare provider industry may not realize that insurance companies, pre-HIPAA, were already subject

to pretty stringent rules regarding healthcare privacy. While it's similar to HIPAA, there are certain, more stringent rules. For example, the Illinois act requires us not only to amend protected health information that may be wrong or written down incorrectly, but it actually requires us, in certain instances, to correct or delete, which means changing the data.

So if you've been in all these HIPAA presentations, and someone asks, "well, does that mean we have to correct the data or delete it?" and I say, "no, you just have to amend it," well, in Illinois there may be circumstances where you have to correct and delete data if you're a health insurance plan.

Now, I want to make a distinction here between health insurance and [the] administration of health plans. Most health insurance companies, while they do provide health insurance on a premium basis to large groups in employer group health plans, they also provide another service, which is administration of self-funded plans. Mostly this involves administration of ERISA group health plans and the question is, does the Illinois Insurance Information and Privacy Protection Act cover a health insurance company when they are not providing premium coverage but when they are, indeed, [in the] activity of administrating health plans. The Health Insurance Information and Privacy Protection Act is part of the Illinois Insurance Code and in many instances, it is a position of many insurance companies that the insurance laws in the various states do not comply with plans that are self-administered because of ERISA preemption standards. ERISA preempts state law, so self-administered plans should not be subject to state insurance laws. We have fun discussions with the Department of Insurance about that.

Now, also in terms of health plan use of data, we are required, when we deny insurance, to provide the individual, the applicant, with the reason for that denial and we also have to provide what we may consider personal and privileged or proprietary information if that information was used to deny the individual health insurance. [We must also] write decisions to cover a number of [other situations as well, including] termination of insurance or the charging of a higher rate to someone because of a greater risk; we [must] provide that information to the applicant. There is one exception. We do not have to disclose privileged information if we deny an individual applicant because they may have had a history of certain types of criminal activity or fraud or they were involved in other scams to misrepresent their health background and health insurance. Also, we do not have to provide medical record history directly to the individual. We provide it to the physician and we leave it [up] to the physician to disclose it to the member; it's very similar to the Clinical Laboratory Act. Those who are familiar with the Illinois Clinical Laboratory Act know that as an individual, we cannot directly get your test results. They're provided to our physicians.

This is the same with how we have to handle medical record information in the context of adverse underwriting decisions. Now, similar to HIPAA, under the Illinois act, we can disclose protected health information to our business associates, but it's limited to insurance transactions, and insurance transactions are only those to other insurers, self-insurers or to business associate-type entities and for other circumstances when it's required by law.

The Illinois act is more stringent in that a health plan may not disclose [information] without an authorization to flexible spending accounts. Now, some of you may be familiar with flexible spending accounts. [T]hey are an employer-sponsored program where individuals or the employer may contribute funds to it on a tax-free basis. It can be used to cover health care that your health insurance doesn't cover. Now, a lot of health insurance companies, even those that serve as health plan administrators, don't operate flexible spending accounts. [Much] of [the administration] is done by banks, bank subsidiaries, and consultants. So in order for this flexible spending account to work, we, the insurance company, have to provide information to the flexible spending account of what is not covered. So there's a type of coordination of benefits, [and] we call it crossover information. In Illinois we cannot provide that information to a flexible spending account without an authorization. But under HIPAA, a flexible spending account is a covered entity, so no authorization is required under HIPAA for a health plan or a self-insured plan to transmit information to flexible spending accounts. So if you're trying to operate an organization on an enterprise-wide basis and you're dealing with a lot of different states and most states do not have this type of law (Illinois Insurance Act), it means that you have to apply one set of rules for one state that you don't have to apply to all the other states. One question that you might ask is whether ERISA self-insured plans are subject to this same rule. Again, it's the Illinois Insurance Act as an ERISA self-funded plan. It should be exempt from Illinois insurance law.

Also, in Illinois, authorizations in the health insurance world have a 12-month expiration date; whereas, under HIPAA, you don't necessarily have to have a time frame. It can [either] be an expiration date or an expiration event [that] can be beyond a twelve-month period. So now here we have to get authorizations for things like flexible spending accounts or you may get authorizations for other reasons to share information with other health plans, and do they have to be renewed every year? They don't under HIPAA, but do we have to do that in Illinois? Do we need to do that differently in Illinois than we do it in Texas and New Mexico or does Aetna need to do it differently in Illinois than it does on a nationwide basis? If you take compliance very seriously and you're very conservative, then the

[different] authorizations must be obtained, but many health plans are not as conservative in their application of privacy laws. Again, do we have to apply that when we're dealing with self-insured ERISA plans?

Now we get to a different set of stringent laws that really can provide complications for the secondary use of data. When I asked Dr. Kizer the question whether healthcare operations is a secondary use of data, you know, he indicated [that] that is one of the ones that may be positive, it could lead to quality improvement. But there is a set of medical information that, even though HIPAA permits a health plan or a provider to share protected health information for certain payment and healthcare operations, under state law, consent is required. [O]ne of those areas is the area of mental health and developmental disabilities. In order to disclose mental health information in Illinois you need to have the individual's consent. Further, you need the individual's consent if you're going to turn around and re-disclose it.

So what does that mean for a health plan that has a business associate or a health plan that's being audited by a behavioral health vendor to see how they're administering mental health benefits? Do we need to get an authorization for that type of healthcare operation? Well, here, the Illinois insurance law [does] health plans a favor, one area where we're given some discretion. In Illinois, insured premium groups may share mental health information with their business associates for underwriting, claims payment, coordination of benefits, health plan coverage, and service decisions.

Does that include all healthcare operations? I'm not sure, but, many of you also administer self-insured plans and ERISA-funded groups, and for ERISA funded groups, we don't have that leeway in providing it to us under the Illinois insurance law. How do we, with all of these electronic information systems, deal with this bifurcation of the law? It's very challenging and it's very expensive and there are a lot of practical implications in terms of the administration of health plans, self-insured plans, and research where we're trying to pull data to understand where there is a great risk of certain types of diseases in the population. It really provides a great challenge.

One of the things that Dr. Kizer mentioned was that one of the costs that is being added to health care is legislated healthcare maintenance. So dealing not only with HIPAA, but all of the fifty state laws, adds incredible cost to the administration of health insurance in this country. [A]t the top of that, as of December 1st, which was only four days ago, we now have the new federal rules of e-discovery. As you know, health plans can be in a lot of lawsuits and now we have to deal with e-discovery. Hospitals, which are large organizations, are being sued. They're going to have to deal with e-

discovery. So on top of HIPAA, you have to deal with e-discovery. [T]hen on top of e-discovery, you've got to determine whether you have some of this sensitive health information like mental health information or HIV or AIDS information.

In order to disclose HIV-related information, it requires the consent of the individual. There is no disclosure without authorization, [and] no redisclosure [without authorization]. If you're a member, under HIPAA, when a covered entity requests medical information, you can treat it as a routine request and you can assume that it is a request for the minimum necessary information. When there is a request relating to mental health information, HIV and (later we'll see) genetic information, these are not to be considered routine requests. They have to be looked at on a case-by-case basis. Of course, you know, we can always deal with this information by de-identifying it, but that's an expensive process as well. So from a health plan perspective, how do we conduct our payment and healthcare operations when we have to really parse out different types of sensitive health information?

Now, many of you may not know, but in Illinois there is a Genetic Information Privacy Act, not part of the Illinois Insurance Code, and it really is directed to health insurers, [who] are prohibited from using genetic information for underwriting purposes. There is one exception, and the exception basically requires that the individual voluntarily disclose that information and asks you to use it, so I would think that you would always have that leeway. But genetic information is something that's coming up more and more in medical records. And while we can use it to some extent for certain payment and healthcare operations, we are prohibited from using it for underwriting purposes.

Now, I'm going to change gears a little bit because basically, we've been dealing with healthcare privacy laws, but health insurance companies are considered financial institutions under the Illinois Personal Information Protection Act, which protects Social Security numbers, credit card numbers, [and] drivers licenses. [W]hat the law provides is, if there is a security breach by data collectors, the individual must be notified of a security breach.

Now, under HIPAA, if we inappropriately disclose protected health information, which includes an individual's Social Security number [or] credit card information, that's all protected health information if we obtain it through our application process [or] our payment process. If we inadvertently disclose it, we do not have to report that to the member under HIPAA. Under HIPAA, we just [have] to do a disclosure accounting and our business associates notify the employer. We don't have to notify every individual.

Well, under the Illinois Personal Information Protection Act, data collectors must notify individuals when there is a security breach, and there are two types of data collectors. [T]his really hits home with health plans and health administrators. There are data collectors that own or license personal information and that would include a health insurance company that provides fully insured benefits through premiums. [I]n that case, a health insurer must notify the resident in the event of a breach of a security system even if it is unlikely that the individual's information will be stolen.

If you're acting as a third-party administrator where we don't own the information—third-party administrators are considered to maintain personal information—then we only need to notify [members of] improper disclosures of Social Security numbers or personal information if there was a security breach and it's reasonably believed that someone may have stolen that information. Breach of security system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.

So the question is, if one of your employees has a laptop and it has a lot of healthcare provider information or health information, is the loss of a laptop a security breach? Well, it's debatable. But if, say, we take a conservative approach and loss of a laptop or loss of the data is considered a security breach, [i]f you're a health insurance company that provides fully insured benefits, you've got to notify everyone who you may know has data on that laptop. The fact is, it's very unlikely, with the kinds of security that at least HCSC abides by, it is impossible to get into the information in someone's laptop. I mean, the information self-destructs, basically, if someone unauthorized tries to get into it. So here if a laptop is lost and you're concerned of a breach in the security system data and you're a health insurer, you've got to notify all of [the individuals]. It could be thousands of people. But if you were a self-administrator, we know it is unlikely that that information has been stolen. It's impossible. We know that and we don't have to notify anyone. We may have to notify the employer, but we don't have to notify those thousands of people.

I just wanted to mention something briefly about marketing and research. Basically, when HIPAA was finalized, they really strengthened the need for authorization from marketing, but you may recall that no authorization is required for face-to-face communications or when we give a promotional gift of nominal value to a client or a member or a patient. However, under the Illinois Insurance Information and Privacy Protection Act, we are engaged in face-to-face communications if we provide you with a promotional gift. [S]ay we're involved in face-to-face communication that's part promotional, part survey, [and] part quality improvement. We need to notify the individual of the questions that we're asking that are

designed solely for marketing or research purposes. So I think that that's an additional requirement on health plans in the collection of data that are not on other types of covered entities such as healthcare providers.

I also want to briefly mention the Federal Electronic Communications Privacy Act. This act, as well as the Illinois eavesdropping statute, prohibits the use of recording devices or what they call eavesdropping devices, basically recording telephone communications. In Illinois, as well as under the federal statute, there's a business use exception, but that really only applies where you are monitoring telephone conversations because you want to be sure your employees are not misusing electronic communication systems. Under the federal rule, interestingly enough, you can record conversations if you're not using it for a business use but you're using it for other uses such as surveying or marketing.

Under the federal rule, there's an exception if only one party consents to do recordation. So obviously when we're a making the call, we're consenting to the recordation of the conversation, but the individual subject to the survey or marketing questions has not, [and therefore] under the federal rule, that's permissible. However, under the Illinois law, all parties must consent to any kind of recorded telephone communication. In fact, there was a long period of time where even in Illinois, under the Illinois law, it was unclear when [only] one party consented if you could record the conversation but now [the requirement is that] all parties [must] consent. For the most part, I know that if you call Health Care Service Corporation or most any other health plan, it's a customer service call. You're always notified that it may be recorded so that you have the option to opt out of that type of call. [B]asically, we've taken a pretty strict policy that parties must consent to any type of recordation of calls to avoid any kind of problems with the ambiguity under federal and state laws.

Also, you may be familiar with the do-not-call lists. [H]ealth plans engage in marketing, as well as a lot of other entities and it's against the law to call, for marketing or survey purposes, any individual who has their number on a do-not-call list. If you're marketing or surveying, you have to proactively obtain those do-not-call lists. Well, what if we make a mistake? Are you going to be subject to penalties? Basically, the law provides a safe harbor that if you didn't implement certain policies and procedures, like getting updated do-not-call lists, getting operating procedures in place of the people doing the calls and you put together these procedures, even if you have made a mistake and used someone's number, you're not going to be penalized under the law, but you have to have those policies and procedures in place. As health plans, we have policies and procedures that cover this type of issue just in case there may be an inadvertent use of a number on the do-not-call list.

Now I'm going to switch gears again and we're going to look at the impact of HIPAA and state laws on data requests to providers. My focus really is going to be on pay-for-performance [PFP] programs that recognize and reward physicians for providing quality care, efficient service, and these programs really require extensive data collection and reporting. Whether under HIPAA they would qualify as healthcare operations, it's not clear to me. I know that quality activities qualify as healthcare operations where you can use and disclose protected health information without an individual's consent or authorization.

I can tell you that Health Care Service Corporation, while we have looked at PFP plans, we do not have any in place right now, but we know that some of the other plans and some of the other group plans in the country and some of the for-profit plans, which we are not, have implemented pay-for-performance programs and they really raise a lot of issues regarding some of the other laws that we've talked about today.

Now AMA has already issued guidelines for PFP programs. They've set forth a guideline that all of the data be administrated in a manner consistent with HIPAA. Also, the AMA has guidelines that the program has an appropriate security program in place.

So in terms of HCSC, we definitely have a lot of the privacy and security programs in place if we were to undertake a pay-for-performance program, which we are not so far. Pay-for-performance programs focus on a number of different types of diseases, hypertension, depression, diabetes mellitus, and you can go on. I'm avoiding saying the ones that I can't pronounce.

Implementation of pay-for-performance programs is going to require clinical research. [C]linical research, if conducted in the context of an institutional review board or a privacy board, [and] if this pay-for-performance research is conducted in that way at least under HIPAA, you will not need the authorization of the individual to use or disclose the individual's protected health information. If you want to implement a PFP program, [you will] get into customer satisfaction, which may include surveys, includ[ing] recorded surveys. So we have to look at how HIPAA and other state and federal laws will affect any efforts to institute a pay-for-performance program.

One of the big areas for pay-for-performance is geriatric medicine because it's one that can be [prone to] overuse of lab tests and physicians get paranoid about medical malpractice. [W]ith [respect to] older patients [and pay-for-performance programs], geriatric research really is going to focus on falls, cognitive screening, functional assessment, end-of-life counseling, osteoporosis, and medication review. So if we're trying to deal with a pay-for-performance program, we want to do research in the area of functional assessment and cognitive screening. We're going to be dealing

with mental health and disability issues. [W]hile we may, under HIPAA, be permitted to use that information without an authorization, at least in most states we're going to need the authorization from an individual if we want to put together a pay-for-performance program that focuses on geriatric medicine.

The same would [be true] if you're doing a study on patients with immune deficiencies. Many patients with immune deficiencies have HIV, so any type of [disclosure of that] data requires certain authorizations. HIPAA does provide sharing of protected health information, but it limits pooling data for research purposes because, if you look at HIPAA, it permits the sharing of PHI for healthcare operations. But in the context of healthcare operations, the covered entities have to have a relationship. They all have to have a relationship with the individual who is the subject of the research.

We're pooling data of a lot of different physicians where, if we have an IPA [Independent Practice Association] and they want to pool data, it's not one entity. They don't have relationships. They don't all have a relationship with the same individual. So that does not fall within the context of healthcare operations if you want to argue that pay-for-performance studies fall within healthcare operations. It limits your pooling of data as long as all the covered entities involved within the research have a relationship with the individual. Of course if you don't [have the relationship], there are other ways of approaching this where you don't have to get the individual's authorization. You can de-identify the data, which can be very costly, depending on the population size you're dealing with, and you can also enter into limited data sharing agreements.

So if you're a health plan involved in any type of use or disclosure of data for a secondary use, what do we have to do? What do we do? Well, first we look at what the law permits. [T]hen we determine the privacy rules that apply under the state department of insurance and then we have to wrangle with bifurcating our premium plans, fully insured plans, and our self-administered plans. We have to revise all our policies and procedures and authorizations to take into account more stringent state law. If you are a nationwide health insurance company, can you use one form [to] fit all? You know, we want to cut down administrative costs. We want one form [to] fit all.

Well, what if one state requires that for a certain disease you need to have a witness on the authorization? There are no lists like that. So [operating] on an enterprise basis could be a real challenge. And you have to take a look at other federal and state requirements that may impact our research design and research purposes. Are we recording? Are we doing marketing? And if we're doing marketing, does the state insurance law

require specific disclosures that HIPAA doesn't require? If we're doing research for pay-for-performance and we're involved with the premium clear plan, do we have to be wary of certain disclosures that may be required under state insurance clause? So it's a talk about adding costs to health care. The one thing that I say is that I am benefiting from some of these healthcare laws because if it weren't for them, I don't know what I would be doing right now.

One thing I didn't talk about and I thought was important to mention, is that there are ramifications for violating state privacy laws. I thought, well, I talked about violating state privacy laws and what does it mean? Under the Illinois Insurance Practices Act, the Medical Health and Disabilities Act, [and] HIV and AIDS [laws], they all create a private right of action where they get individual damages [for] a prohibited disclosure. So we have a greater level of liability under the Illinois Insurance Privacy Act, never mind dealing with mental health, HIV, [and] genetic information. [A]ll of these violations can constitute a criminal activity involv[ed] in fines ranging from $20,000 to $100,000. So compliance with these laws is important not only for our members, but also to protect our own corporate liability.