RECORD, Volume 29, No. 2*

Spring Meeting, Vancouver, B.C.
June 23–25, 2003

Session 65PD
HIPAA Regulatory Update and Implementation Issues

Track: Health

Moderator: KARA L. CLARK
Panel: BETTY HAYNES†
STEELE R. STEWART
STEPHEN P. WOOD‡

Summary: Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance is upon us! The panelists address new HIPAA-related concerns for health insurers, such as:

· The status of implementation issues
· Privacy
· Transactions and code sets
· Employer identification numbers
· The impact of privacy and transaction code set rules on actuarial data
· An update on current developments relative to the pending rules

Attendees gain a better understanding of the current status of HIPAA implementation and learn about the direction of outstanding HIPAA issues.

MS. KARA CLARK: I'm the health actuary on staff at the Society of Actuaries. One of the volunteers in the health area on our education and examination

*Copyright © 2003, Society of Actuaries

†Ms. Haynes, not a member of the sponsoring organizations, is national director of legislative and regulatory implementation at Humana.
‡Mr. Wood, not a member of the sponsoring organizations, is managing principal at Reden & Anders in Chicago, Ill.

Note: The chart(s) referred to in the text can be found at the end of the manuscript.

committee told me a story related to HIPAA, which I think is a good illustration of why we're all here. He's a consulting health actuary who was engaged by a client to do a large claim study. They got the data report from the client, which included some of the information you would expect, such as Social Security number, which was blanked out; name, which was blanked out; and diagnosis as well as paid claim amount. When they were reviewing the data that they had received, they saw that there were some mismatches between the diagnosis and the paid claim amount. In some cases the diagnosis that was indicated had a claim amount that seemed extremely high relative to that diagnosis and vice versa. That seemed inconsistent to them, so they went back to the client and asked about that inconsistency. The client said that because of privacy concerns, they scrambled the paid-claim dollars. So that's why we're here--to talk a little bit about HIPAA, what it means to you and your work as an actuary, what it means to your organization and what it may mean to some of the other organizations with whom you work.

Our panel is well versed in this particular topic. Betty Haynes from Humana is the national director of legislative and regulatory implementation, In this position she provides strategic direction to all Humana functional areas affected by both state and federal regulations to ensure successful implementation in operations. Betty has also acted as the program director for HIPAA implementation, where she was responsible for planning, development and implementation of the HIPAA regulation. During her 15-year tenure with Humana, she has gained significant experience in the health benefits industry, specifically in commercial HMO, PPO and Medicare risk contracting through her roles in compliance, finance, provider contracting and sales. Additionally, during her career she has been the director of operations for a very large marketing services organization (MSO), as well as a consultant to the Centers for Medicare & Medicaid Services (CMS).

Steele Stewart is an FSA with more than 15 years of experience as a health care actuary. For the last three years, he has been a director of actuarial services at Blue Cross/Blue Shield of Kansas City. Prior to joining Blue Cross/Blue Shield of Kansas City, Steele had 12 years experience as a managed-care consultant with Towers Perrin and Deloitte and Touche. He has expertise in large and small groups, Medicaid, child health and Medicare Plus Choice products and provider contracts. He has consulted with HMOs, PPO plans, Blue Cross/Blue Shield plans and hospital and health systems. His expertise on this topic stems from representing the Blue Cross Actuarial Department for the implementation of HIPAA at Blue Cross/Blue Shield of Kansas City.

Steve Wood is the managing principal with the Reden & Anders Health Care practice in Chicago. Prior to his current position he was a principal with Tillinghast Towers Perrin, where he led the firm's senior services practice. Before joining Tillinghast Towers Perrin in 1995, he was the managing director of Strategic Consulting Services at the Blue Cross and Blue Shield Association. His work has involved the impact of HIPAA on insurance and provider operations. He has more than 20 years of health care experience in a variety of positions. Prior to joining the Blue Cross

and Blue Shield Association in 1986, he was a specialist in hospital capital financing at the American Hospital Association. He also spent three years as a finance director and director of patient accounts at large medical group practices.

Betty is going to start by giving an overview of HIPAA. Then Steele will follow and speak on the impact of HIPAA within his company and within the Actuarial Department and, finally, Steve will follow with an external perspective, looking at the implications of HIPAA on your organization's relationships with other organizations.

MS. BETTY HAYNES: I'm hoping to provide you all with a basic understanding of what the HIPAA regulation is.

What is HIPAA? It's the Health Insurance Portability and Accountability Act and it was put into law in 1996. The first part, which was Title I, dealt with the renewability and portability of health care coverage. Then came Title II, administrative simplification. As I start to go through the presentation, you'll see that it's anything but simple.

Basically you have HIPAA and you have Title I, which deals with portability of insurance. We're not going to cover Title I because everybody should have complied with that at this point.

Title II is the portion we're here to talk about.

Title II. Initially it started with the electronic data interchange (EDI). The intent was similar to that of the banking industry. It was to standardize communications. Providers were sick and tired of using different forms for all of the different companies. The federal government put the privacy law out and then the regulatory agencies interpreted it and put out a regulation. The privacy law had 1,400 pages and they interpreted it and brought in the American National Standards Institute (ANSI) to set standards and guidelines on how to implement it.

It's taken years to get us to this point. The first thing that they said was, "Let's define which transactions we want to set standards for." They were the typical ones that are used in the health care industry. They included the claim, whether it's a hospital claim, a UB92 or a HCFA 1500, enrollment and disenrollment, remittances, authorization and inquiries.

Obviously this is a good thing because now at least as you're receiving information, it's all going to be standardized. The first thing they did was to standardize these types of transactions that occur electronically. When they say standardized, they mean for the claims. One, it's going to have 40 fields and field No. 1 is going to be name and it's going to have 40 spaces, etc. They basically went through and did that for each one of these transactions. Then they decided that within those transactions there are certain code sets that they want to make sure also get

used. So, they added the code sets piece. The code sets piece is everything from your ICD-9 for your diagnosis to your CPT-4 codes. If you think about it in terms of HCPCS, you have the Level Is, which are CPT-4s. You have the Level IIs, which are more for ancillary type of services. Then you have the Level IIIs, which are homegrown codes. Those go away. You're not allowed to use them any more. You can only use the Level I and Level II.

It also set for dental, CDT-2s, and they have the ability to issue revisions. ICD-10 is up and coming, so systems are going to have to change to be able to handle the new diagnoses codes when they actually get published. This is a never-ending regulation.

Then, last but not least, they decided that as they were doing this, they should go ahead and come up with unique IDs. The regulation defines plan IDs, provider IDs, member IDs and employer IDs. One thing I do want to caution you on is that we don't have final regulations except for the employer ID ones. Supposedly, the provider ID regulation is going to come out in September 2003, and for member IDs, you get what you ask for. What you'll find is you'll have a lot that gets put out there and then the regulation comes out and the groups that wanted the regulation or the law come back and say they don't like that. The member ID is on permanent hold, because people started to hate it. They do not like having their Social Security numbers used. So, what do they come up with? As you transfer from Humana to Blue Cross to Aetna, you'll have one ID number and that way it all follows you. Then people started saying, "that's Big Brother watching me again. Now I not only have to memorize my Social Security and my driver's license number, you're going to give me another number? I don't think so." All these groups came out and said they didn't like that one. So, it was put on hold for now.

That's basically what occurred. They tweaked and they added to this regulation a privacy act and they said as you communicate all this, you need to protect it. The privacy regulation says you have to protect personally identifiable health information. When they originally wrote this regulation, it really only applied to electronics, but that's been expanded to encompass everything. The mode does not matter; it has to be protected. They came out with this security and asked, "How are you going to protect it?" Then they came up with regulations around how you have to protect that information if it's transmitted electronically versus if it is transmitted in hard copy paper, fax, etc. That's basically the administrative simplification piece of HIPAA.

Chart 1 shows the compliance timelines by regulations. These dates change quite often. We are supposed to be complying with the transactions and code sets in October 2003 (originally October 2002). I was on a conference call several weeks ago with our trade association, as well as CMS, and they were saying that many small providers might have some sort of waiver so they can go beyond the October date and that we health plans need to be thinking about contingency plans so that we can accept those as standard in October.

We're thinking national provider identifier compliance is going occur in September, but we don't have a date yet. We have to comply with the employer ID by July 2004. The member ID one is on hold and I don't think it's ever going to get published. We also do not have a date for the health plan identifier. For privacy, you should be compliant already. We needed to be compliant by April 2003. The only exception to that is for small health plans. Small health plans are defined as health plans with less than five million in receipts. They don't have to comply until April 2004. For security we don't have to comply until 2005. The problem is, in reality we had to comply by April 2003. If you've identified what you have to protect and then you don't protect it, it could be problematic. We went ahead and complied with the proposed security regulation. Once the final came out, it was pretty similar. There really wasn't much difference, so you had to comply with security in order to be able to comply with privacy.

I'm going to focus on the privacy piece of the regulation. What is health information? It is any information that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that is either oral or recorded in any form or medium. It relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

What information can define a person? It's not just your traditional main Social Security number. Chart 2 is a listing of some of the different things that can be attributed to a piece of health information that makes it identifiable.

What is protected? Individually identifiable health information and protected health information (PHI).

Now we'll define what is protected. I'm going to tell you what you can do with it. You can either use that information internally or you can disclose it externally. You're allowed to use and disclose that information for three purposes: treatment, payment, and health care operations. Chart 3 shows some examples of uses and disclosures.

Chart 4 shows some examples of health care operations and these are obviously just about everything involved with paying a claim. On the front end, from the utilization management activities that might occur to determining whether it's medically necessary, to issuing referrals, to giving the services, paying the claim and so on. Then there's also all these other things that health plans, for example, do. It is your quality management activities and conducting the regular day-to-day businesses, such as administrative processes that you have to do in order to run your health care operations. It's the law department, for example, doing the functions that they do in providing guidance to, for example, grievances and appeals. It's all the other functions that occur in your organization that are necessary in order for you to run your business.

What is payment under HIPAA? They are activities undertaken by a health plan to obtain premiums or provide reimbursement for the provision of healthcare. Again, it's everything on the front end from determining if a person is eligible, through being approved for a service. Obtaining that service is obviously treatment. That is not performed by us as a health plan, that's performed by the provider. On the back end is the receipt of that claim, paying that claim, adjudicating it and actually issuing a remittance.

If you want to disclose information for purposes other than treatment, payment or health care operations, you have to de-identify it. The regulation issues instructions so you know which pieces of information you need to remove in order to make it de-identified. If you de-identified the name and the Social Security number and all that was left were diagnosis and amount, you have no way to track down who that person was so there is no real reason to scramble the paid amount and the diagnosis.

If you want to disclose that protected health information and you don't de-identify it, then you must get prior consent from a member or a patient. In order to do that, there are some steps that we have to follow.

We have to issue an authorization form. That authorization form is going to detail for that person why we want to disclose that information and whom we're going to disclose it to. That same form will ask for their permission to do it, and they must sign it and date it. We also must give them instructions on how they can revoke that. Humana has chosen, in our particular case, to make this only good for 12 months. This states that everybody must follow HIPAA in all 50 states. However, if your particular state has requirements that are more stringent than HIPAA, then you need to follow those. We're in 42 states so we took the one that had the shortest time span and for us it was 12 months. There are certain states that allow you to do 18 and 24 months. If you have a pharmaceutical company that would like information for a large group, the only way that you would be able to access that pharmacy data from a pharmacy benefit manager (PBM), for example, would be to get consent from all of these people.

Many things fall under some type of health care operation, so it's okay to go ahead and disclose that information. But, for example, if you have a pharmaceutical company that is performing a clinical study on a drug and they want to know all of our females that are age 50 and over that have had breast cancer, that does not qualify under health care operations. So, we would need to identify who all these people are, send them this authorization form and have them sign that authorization form before we could release the name of that person to that pharmaceutical company.

Business associates. In the case of a disease management vendor, we're allowed to use and disclose information for purposes of treatment, payment and health care operations. Often health plans will hire vendors to do certain things whether

it's assistance with benefit coordination or whether it's recovery or disease management. We'll hire external vendors to assist us with those functions and that's allowed. The regulation states that in order for you to be able to hire these vendors, you must have a business associate agreement with them. Our business associate agreement, for example, is approximately 13 pages long and binds them to all of the same types of requirements that we're held to with this HIPAA regulation so that they can't use or disclose that information for any purposes other than what they have been hired to use that for. This even applies to auditors, so if we hire someone to come in and do some work for us, we'd have them sign one of these business associate agreements so that they in turn can't take any information that we provide them and sell it or use it or disclose it.

As if this regulation wasn't invasive enough, it also describes that when you're doing your job, whether you're going to use the information or disclose it, you need to use or disclose the minimum necessary amounts. Every time you perform an activity, you must make sure that it's the minimum necessary. For example, if you're going to send out a report to this disease management vendor and they review all of your congestive heart failures, all you can send them is a listing of those people who have congestive heart failure. You need to limit it to what they have been specifically hired to do for you.

The regulation also requires that every patient and every member receive a notice of what their rights are. Our notice explains what we do, how we protect their information and what rights they have. They have the right to object to regular disclosures that we would do during the course of business, but we're also given the ability to deny their objections. They have to bring all of these requests to us if they want them and then we review them and determine whether it's something that's feasible or not. They have the right to request restrictions on who can see their information. They have the right to access, review and amend their protected health information. They have the right to complain about our privacy policies and procedures and they have the right to alternative communications. If they file any of these complaints against us, or any of these requests, we cannot intimidate or retaliate against them.

We see alternative communications coming into play. One thing that we had to do, for example, was to send anything that's related to Health PHI, and for the most part that's going to be the explanation of benefits (EOB), directly to the actual person who receives the services rather than to the subscriber. This was Humana's interpretation of what we felt we had to do in order to protect privacy so you didn't want a spouse seeing another spouse's information. Obviously, for anybody age 18 and under we would still direct it to the subscriber.

If you have a situation where a spouse has received some service that they don't want the other spouse to see, this regulation allows for people to contact us and say, I have a situation where my life is in jeopardy if I receive this at home and so I would rather that you send it to me via fax or that you send it to me at an

alternate address. We had to make arrangements for this. It also allows for emancipated minors. In the State of Florida, for example, if a girl is pregnant under age 18, she is emancipated for that pregnancy. We had to take that sort of thing into account. This is where you see something that's a little more stringent than what HIPAA requires, so we had to take the state requirements into account.

Part of the reason for this wasn't just the fear of identity thefts. If I'm up for a promotion, do I really want my employer to know that I am receiving treatment for cancer? Probably not. One of the things that this regulation does is ensure that there are firewalls set up, that information can't be shared. In the fully insured environment, we should have never really been sharing that kind of information. It should always have been de-identified, but this takes it a step further and, in the self-funded environment, really ensures that information is not going from the employer's side of the house to the health plan side of the house. This is actually a good thing. Another thing is, if I'm applying for a mortgage do I really want my mortgage company knowing that I'm receiving treatment for cancer? Probably not. Part of what this does is to prevent information from being handed out so we don't get penalized because of our health status. The agency that's going to be responsible for monitoring this is the Office of Civil Rights, so it goes hand-in-hand with disallowing discrimination against me for my gender, race or religion. Health status flows right in there.

From a privacy perspective we had to put several things in place. First, we had to designate a privacy official and a privacy office and in ours alone we have about 14 people to deal with all the requests and things that are coming in. We had to define the uses and disclosures of protected health information. Every functional area in our company had to develop procedures on how it used the information, how it disclosed the information, for what purposes, etc. We also had to define when there would be uses or disclosures that don't fall into treatment, payment or health care operations that would require a consent from the person to allow us to use it or disclose it. We had to issue the privacy notice and continue to issue that privacy notice for any new members that come on board and then every three years afterwards in case there's a change in our privacy practices.

We had to develop amendments for our existing vendors and providers, for business associates, for those that perform a function on our behalf. We had to implement privacy procedures to safeguard all of the members' PHIs.

Security. Obviously as we're defining how we can use and disclose protected health information, we had to put in all of the different types of safeguards. Chart 5 shows administrative, technical and physical types of safeguards to ensure that that information doesn't wind up in the wrong hands.

Charts 6 and 7 show penalties that were issued with this regulation, and these penalties are quite severe in nature. From the EDI perspective, every time that a provider or a vendor submits a transaction and it's not in the compliant format,

they could issue a fine. As I spoke earlier, I think there's a lot of concern among the regulatory bodies that providers and vendors and clearing houses aren't going to be ready to do these standard transactions, so they're already talking about issuing some waivers if they're not ready by that October 2003 date. These penalties come up quite rapidly.

The penalties for privacy range from one to 10 years of imprisonment and from $50,000 to $250,000. The first one, which is the $50,000 fine and not more than one year, is where you might do a mailing and on that mailing, when you ran the labels, you included all the diabetic people that were getting the diabetic brochure and it was a mistake. That's more of a you-didn't-really-mean-to-but-it-happened and you didn't follow procedures for how you scrub information to do the labels, for example. That would be an example of No. 1. An example of No. 3 would be to run a report of all your diabetic patients for a pharmaceutical company so the company gives your sister a job. It's something that would be for personal financial gain. Another example would be if I were trying to hurt somebody. If I found out that Suzie Smith is having an affair with my husband and I have access to her health information and find out she has diabetes, and I spread rumors out there. Those are the two examples of either for gain or for intentionally trying to hurt somebody for which you could look at severe penalties of 10 years in prison and/or a $250,000 fine.

High level deliverables. We modified our provider and vendor contracts for trading partners and business associates as applicable. We identified the uses and disclosures that fall outside of treatment, payment and health care operations so that we could implement procedures to comply. This was actually the most difficult part that we faced because we had to actually go department by department. We spent almost two years working on that piece to identify all of those reports. We also developed policies and procedures to comply with all three pieces of the regulation.

We developed and implemented security measures. We actually ended up putting little slide cards on each one of our floors to make sure that people only accessed the floors that they needed to. We remediated and migrated information technology platforms so that we could deal with the EDI portion of this regulation. We conducted training on all of our policies and procedures company-wide based on the Web so that we could track that everyone took these. We gave everyone about a three months' time period to get it done. Again, we developed and mailed the member privacy notice.

MR. STEELE STEWART: How did this whole thing get started? I've got a Beltway legend for you. Senator Smith was in the Capitol and Pharmacy Company XYZ gave him a call on his cell phone. The company tells him it is aware that he's taking so-and-so and it has another drug that it would like to introduce to him. Senator Smith said, "Who are you?" He had no idea. "How did you know that I had that condition? Who are you? Where is this coming from?" It's an urban legend. There may be

some truth in it. I don't know if anybody knows if this is a true story or not, but the point of it is that PHI came to somebody and got them scared. On one hand, if I received that phone call I might be a little bit nervous about it, but on the other hand, I might ask, what's that other drug? That's my style. But as a result, it started shaking things up. There are many details in the health care industry. Information is our lifeblood. Basically what this legislation has done is added additional information to all the information that we already have that needs to be tracked. With that, I'll start with some of the impacts on our plan.

My presentation will start with a high overview and then I'll talk about the actuarial department and the underwriting department. First of all, we started the implementation about two years ago. The individuals that were involved did an excellent job with weekly meetings, a full project management schedule and whatnot. They talked with the Blues' Association. The reality is that there are different interpretations of how HIPAA should be implemented and you'll see some of the things our company handles differently from Betty's.

The most significant is the handling of medical records. For our organization, we considered that medical records are the ultimate PHI.

The impact was across the board. We had to look at all our policies and procedures, but I won't repeat it because Betty touched on that same thing.

We had to develop new processes to assure security of PHI. I'd say there are three big legs that this regulation stands on. What is PHI? Who is using the information within the organization? How is the information disclosed outside the organization? In some ways it's a simple concept. We have disclosures to external parties and uses by business units.

For disclosures, we have contract holders and members. One of the decisions that we made was to treat every member equally. The information always goes to the member. Any PHI goes to the member, whether it's a child or an adult. It's all standardized in that way, but it can go to different addresses. For business associates, we have a business associate contract. Ours is only about three pages long, but I think it's just as lethal so you have to watch out for it. I'll give you an example. We have agents, brokers and vendors, such as actuarial consultants, and we want to authenticate the other party.

Every job position defines needed use of PHI, from the CEO to the janitor, every position within the entire organization. We went through a process of determining what information that person needs access to because that's what HIPAA was requiring. This is the one part of the law that I think is arduous and really has very little benefit, because it tracks the whole organization in a thought process that doesn't have much value. That is my opinion.

We have tools that we've developed internally: Web support, the systems, the data warehouse and the LAN structure. If a member or a physician is going to send medical records to us, they have a specific blue envelope that goes to a specific post office box. We have dedicated faxes within our organization and when the fax comes in or whenever we send a fax out, we always include an extra page on the top and on the bottom because we don't know where it's going to go. You don't want to disclose the information to another party arbitrarily. It contains somebody's PHI information. There could be a nurse that's not involved with that patient that walks by the fax and notices what's going on with that patient. So to protect that PHI, we fax pages on both sides. We've got carefully managed central files and medical management for all the medical records.

PHI categories. Blue Cross of Kansas City's interpretation is that there are six categories. The first category is demographics: Social Security number, date of birth, ID number, and address. Is address PHI? How does that have to do with health? Technically, it's not PHI because it doesn't disclose what health condition someone has, but it discloses potentially who they are by their address or by their zip code. What we decided in this organization is that we're just going to keep it simple in the sense that any information about a member is considered secure, private information, and that way the mindset is consistent. You don't have to go back and forth. We have demographic information, which is really used to identify the person. The second PHI category is enrollment information, such as effective date and benefit plan. The third category is customer contact, such as notes on phone calls. The fourth category is financial, such as billing claims. The fifth category is claims or application health statements. The last PHI category is clinical information. The actuarial department has access to all of these except for the customer contact information because our job function really requires us to be able to understand what's going on from a risk perspective.

As far as Web support, there has been a large investment in educational process and Web structure. If we want to find out information about an employee, we can find out about them. For every employee within the organization, I can look to see if they are cleared to view a particular PHI category. Within departments there are more comfort levels with knowing who is cleared for what information, but you need to be a little bit cautious in meetings because you may be in a meeting where you want to talk about something with PHI and somebody there doesn't have that clearance.

Impact on most business units. We had to go through training. We should have all had HIPAA training. It took us about two-and-a-half hours to talk through the issues, sitting down at the desk in the actual department. We had to clarify how to communicate about PHI. The biggest issue is having the greatest awareness about what's being disclosed. It's a cultural phenomenon across the whole organization. We also evaluated many policies and procedures and improved our organization.

One of the ways we improved our organization was through the LAN structure. The LAN is very well organized. Every department has its own directory. Underneath every directory there are all of the PHI categories, providing some structure there. Lastly there was additional time and cost, which were definitely impacts.

Impact on actuarial services. Both internal and external disclosures were affected. An example would be sending files to a disease management vendor. We need to secure the files. If it's an Excel file, we need a password to protect it before sending it out.

Treatment, payment and normal operations were also affected. Projects must have a defined purpose that fits within one of these things. If you can conceptually think of what you're doing as fitting within that box, then you can sleep at night.

Impact on external vendors (actuarial consultants). Blue Cross and the U.S. Department of Health and Human Services may inspect internal practices, books and records relating to its use and disclosure of PHI it creates or receives from Blue Cross/Blue Shield. I was in consulting for 12 years and that's your lifeblood. The information that you get from the clients is important and so potentially you need to return all the PHI, if it's feasible, or you need to be able to destroy it upon termination. One way to destroy it would be to get rid of the information that identifies the person.

Impact on underwriting. Small group, direct pay and large group is what we're going to talk about. In the small group market, the director of underwriting said it increased the time that they spent by about five to 10 minutes on an eight-hour day, which is between 1 and 2 percent of their time, doing extra paperwork and putting those extra pages in the fax to send things out. It also cost $1,000 a year for a dedicated P.O. box and they don't see any decrease in costs at all.

Medical records. About 10 percent of the applications for our organization have medical records or they're needed as part of the application process. Before, we called the provider, and really underneath HIPAA as far as we're concerned, we still should be able to call the provider because they're a covered entity. We're a covered entity. We're brothers. We can talk freely and share the information back and forth. But providers tend to see HIPAA differently. Some of them will refuse to share that information. The education process of what's really allowed is not there. We need to contact the applicant or the member. The applicant needs to send an authorization document to them. They sign it and give it to the provider, and that adds about a week to the process. With our schedules it would add more than a week on that. Then again it goes to central file and medical management.

Phone calls. There's a matrix that lists all the different type of questions you're supposed to ask the different parties so that you know the right question to identify whom you are speaking with.

E-mails. E-mails aren't secure. Somewhere out in Internet-land, they could be snatched and somebody could find out somebody's PHI information, so they need to be locked and secured. To avoid that, if you're working with a broker, the underwriter can ask a generic question – a question that doesn't reveal anything about the applicant, but is general enough to get the information out. That's one thing that we'll try to do. For example, the question could be, "you're missing information on questions 1, 3 and 5 on your application. Could you provide more information on these questions?" But if there are specific questions, such as how long have you had diabetes, it needs to go into a Word document, and that Word document needs to be locked and password protected before it can be mailed out. Then the underwriter should be careful not to disclose what's not needed.

Most likely, the underwriters are going to call versus using e-mail. They can talk directly, they can just save the information and it's direct correspondence. The turnout time is quicker than going through these steps unless there are many questions.

Clean desk policy. The only people that are supposed to have access to the information are the people that are going to use it. If you have a desk with PHI information sitting on it, somebody from another department could walk by, see it and pick it up and use it. That should be avoided. In our underwriting department you have to clean your desk and all client member information needs to be secured.

Reuse of PHI. Research is not allowed. That is just huge. For example, as a consulting actuary if you have PHI information for a pharmacy and you want to use that information for research and it's for research purposes only, then you can't do it. When I was in consulting we used the claims data from several health plans to try to get normalized information. This is a great idea for the health care industry where we're all trying to improve everything.

For operational purposes you can use it. The big thing with underwriting is, for example, we have Jane Smith who went ahead and wrote the application out, disclosed all that she thought about at the time and two months later she is submitting another application with none of that information on it. One of the concerns was the way HIPAA reads is that potentially you have to destroy that first application because the purpose of that application was for the initial application process. Another interpretation is that you can hold onto that information and use it for underwriting.

Large group. Claim information is de-identified, therefore there's really not PHI. For example, you get three cancer cases that cost and total a certain amount. The cases are ongoing or over, but HIPAA is used as a means to keep from supplying member information. The impact of one party not disclosing the PHI information is that you get data massaged down into a non-PHI form that cuts off the path, cuts off the work flow and therefore, also changes conceptually. People just don't want

to share information, so we get less information and as a result the rates are potentially more. The underwriters may be more conservative. But because there's no direct PHI, it's not as cumbersome.

MR. STEPHEN WOOD: I'm going to be a little less formal about presenting things to you and talk about some of the things that we've seen in working with a wide variety of plans and plan types and different kinds of organizations over the last three and a half years or so.

When I was with Towers Perrin, we worked with many employers, self-funded employers, on HIPAA issues. We worked with many health plans. We worked with provider organizations. We worked with consultants on HIPAA issues. I think that one of the big mantras is that there is a real danger with HIPAA of overreacting. For the last several years there has been the old Chicken Little syndrome -- promulgated by consultants! Employers are told you can't do anything with health-related information. You can't release information, you can't process information and you can't store the information. Employers ask themselves, then what are we going to do? I think the idea is that you have to go back to what the purpose is and what the intent of HIPAA was in the first place. One of the reasons that the privacy part of HIPAA came into being was not because people generally thought privacy was a cool thing. Who wants their health care information splattered all over the place? But in fact, when you think about a world where you standardized all of the EDIs, what happens if somebody, God forbid, finds out what your ID number is? Your entire medical history is available. The beauty of the health care system in the United States right now, in terms of privacy, is that it's so chaotic and so confusing that nobody can find out anything about anybody. When you standardize things it doesn't matter because now you can trace. That was the whole cry around the privacy rules and the rules got written and there was probably a little bit of an overreaction. I think the intent behind them is unarguable. In fact, when the Clinton Administration released the privacy rules in its last days in office, the Bush Administration came in and said it was going to review these things. They took a look at it and basically within two or three months said there's really not much it could change. This is kind of mom and apple pie. The devil's in the details. The question is: How far do you drill down?

We'll see one or two of those cases where there are obviously over-the-top sorts of sales of PHI for personal gain. One of the standard operating procedures at a couple of plans I worked with, in terms of sharing the PHI, was that every time an individual turned 64.5, they kicked the member's name over to their life insurance company and they shared information back and forth across the subsidiaries under a larger organizational structure. That would send you to jail now, but for them it was just standard operating procedure. They were offering another service. You can bundle your life insurance with your individual health policy. It does make people step back and think about the process they are doing. To be honest, most of the people that we've worked with figure out a work-around. If the process is valuable enough to do it in the first place, you're going to figure out how they can continue

to do it under the rules. Getting authorizations from people is like a nightmare. Trying to ask somebody's authorization for their PHI release is troublesome, because not only do you have to get the authorization, you have to record it, maintain it and keep track of it. Then you've got to log what was released and when they received it and what they did with it. It's not pretty. So people go to extreme measures to avoid their authorized release. There is a lot of shoehorning into payment, treatment and operations.

Steele said something about not being able to do research anymore. That's true. In fact, one of our clients actually shared their claims data with the local university. They did real academic research on it and they didn't have an institutional review board (IRB) or a privacy board for the research function. They couldn't do it that way any more. But for research purposes, for instance, for establishing national benchmarks on normative data and the consultant actuary's lifeblood of national databases, most people argue that it definitely falls under an operational type of release because that's how you're setting your rates. It's not trying to figure out how many days in a hospital a diabetic stays just for the sake of figuring out what the diabetic's hospital stay was worth. You can rationalize a lot of situations.

The Office of Civil Rights at HHS has 50 people regulating this trillion-dollar industry, so I wouldn't lose a whole lot of sleep at night over the big, bad bogeyman knocking on the door telling you that you're going to jail because you violated the HIPAA. Actually, the only thing that they'll send you to jail for is the violation of HIPAA privacy. The transaction format and security pieces are civil violations so you'll just pay money.

More than half of the people here are with health plans. Another third are consultants and a smattering is something else. The fact of the matter is, none of you are what you think you are. When you start peeling the onion here from the HIPAA perspective, you have different responsibilities depending upon who you are. For instance, those of you that are working for such places as Humana and Blue Cross, you're a straight-up health plan. I bet you also process claims for self-funded employers. You are a business associate to that covered entity, so you don't have your health plan hat on. Now you're a business associate to another health plan or another organization. Many larger health plans are also self-funded employer health plans for the employees of the health plan. That's a whole different rule. Or, you're a provider. I know of at least five Blue Cross plans and a number of other plans, managed-care organizations, that don't think they have providers on staff, when in fact, they do. Many employers have providers on staff doing things like worker's compensation review. Some of them are actually even providing medical care.

We found one plan that actually had a whole clinic in the basement for employees, but we got it out from under HIPAA and here's how we did it. They didn't release any EDI to anybody because they only performed the services for the employees and didn't bill anybody for them. If they didn't bill anybody, then they didn't have to

comply. Just think about all the aspects of who you are: providers and clearing houses.

One of the biggest jobs that we did recently was for a large Midwest manufacturer. For an organization like that, the big mantra for the senior executives and for that matter, all of your major self-insured groups is: "Make it go away. I don't want to deal with it, and I'm not going to jail." You heard that over and over again from major employers. Their mantra is "Set up whatever you have to do, I don't care. I make tractors for a living. The last thing I want to think about is HIPAA – I don't want to deal with it."

We found that standardizing procedure and diagnosis codes, in addition to pure IT issues, has a major business implication. Most local codes are created for a good reason. They were created to address a particular situation. Let's say you had an OB group that wants to bundle the entire course of treatment for the pregnancy and they wanted to have one code and you paid them a lump sum. You paid $3,000 for a normal delivery and the code is 112. Well, what happens when HIPAA comes along and says there can be no 112? You've got to bill separately for the initial visit, for the follow-up visits, for the hospital delivery, etc. Guess what? I can guarantee you that it's going to cost more than $3,000.

Here is the other deal. Let's say you've got five local codes that translate into a procedure code. These local codes have all sorts of different revenue amounts associated with them. If you translate this into a standard code, what's going to happen? Physicians migrate towards one code. The physician that was billing on the code at the top, who's revenue code was 10 percent higher than the standard code output, is not going to be happy. It had nothing to do with this service or what he was doing, it just happened to be the happenstance of what he was billing under.

What do you think this guy's going to do? He's not going to just sit there and see his payment revenues reduced by 10 percent. He's going to migrate to another standard code that meets his revenue requirement. Guess what? You messed up both ways. You're paying more because the local code translates to a higher revenue code, and the guy that didn't get the higher revenue code migrated to a different code, so you're out more money. There are some huge implications that you have to be concerned about and aware of.

I want to show you a case study of a railroad company with 120,000 employees west of the Mississippi. The railroads for the last 100 years have really done a lot in direct provision of health care. They have huge worker clinics, they have lots of worker's compensation issues and they're very paternalistic. Most of our employers still are very paternalistic. The amount of PHI flying around this company was mind-boggling. They didn't really even think it was that big of an issue. I'll give you an example of another major employer that routinely did a health care status check on employees' dependents when they were considering an employee for a promotion or a transfer to India, for instance. You don't want to offer a promotion

or a transfer to a person whose son is a hemophiliac and transfer them to some third world country where they can't have access to health care. This employer was making those decisions on behalf of its employees and feeling good about it. What was their reaction to us when we told them that this practice is bad because you're going to get sued if anybody figures out what you're doing here? Their reaction was that they just were providing a service to the employees and didn't want to put someone into an awkward family situation. They were making decisions on behalf of their employees. It happens all the time.

Chart 8 is an example of the types of health information that the various areas have to protect.

Chart 9 shows the number of departments that had direct access to PHI. EAP is huge in terms of access to PHI, return to work and all types of things. They're actually pretty good about that. I'll bet every one of your plans, those of you who are of any size, have some EAP function. That's protected health information. You probably do a good job at it, but thinking about those hats, that's a different hat to wear. All the way down through drug screening and others.

Charts 10 and 11 are two scary tables. They're showing that there are a whole lot of sources of the protected information and how it's being communicated both internally and externally in the organization. It's simple data mapping. The bad part is that you're wondering why you are doing this. Actually, as Steele and Betty pointed out, a lot of this has a very beneficial impact. Mapping helps organizations get together policies and procedures. Additionally, many organizations find a lot of redundancy in what was going on and 14 people were touching the same piece of information when they really didn't need to. So there was actually a fair amount of upside amongst many organizations regarding remediation.

MR. TOM AHMANN: My question has to do with some news that I have seen coming from state insurance departments about disclosure of information to small employers. I think the idea was that small employers are being told their experience is bad and therefore their rates are going up and they want access to information that's causing their insurer to raise their rates. It seemed to me that the insurance departments were going in opposite directions to the intent of the privacy of HIPAA because the classic example was for employees. How hard is it for the employer to figure anything out about what's going on? If you give them anything, they can probably figure out who it is. I'd like comments from anybody on their opinions about those issues.

MR. STEWART: For Blue Cross Kansas City, we're not disclosing anything to the employer, so they may have poor experience and we'll just say it's based upon your poor experience.

MR. AHMANN: If a state insurance department wrote a bulletin and said that you were supposed to disclose, what are you going to do?

MR. STEWART: I would go with the federal law.

MR. WOOD: But this is very difficult. We've seen states like New York where there are cancer registries and things like that which they plan to participate in. On the face of it, it doesn't comply with the intent or HIPAA rules. Most plans, unlike Steele, would probably cave on it. What are you going to do? Are you going to listen to the person in your face or the person off in Washington, D.C.? So you tend to cave. The thing that we advise plans to do is just make sure the state knows what it is asking for and make sure that the other part of the DOI that's trying to enforce HIPAA is also in the know about what their request is and how you're going to package it. You've really got to protect yourself because if that person does lose his job and you've done the disclosing, the state isn't going down. You're going to be subject to the suit. So that's the risk management with respect to it.

MS. CLARK: How involved have your organizations been in helping with education of providers?

MS. HAYNES: About two years ago we started doing quarterly newsletters to the providers, just at a high level, explaining to them what HIPAA was and what our expectations were of what they would be putting in place, but we really didn't dictate what they needed to put in place. A lot of departments felt that really they needed to hire their own attorneys to do that or a consultant to help them. We provided them access to Web sites that are out there from different consulting firms. We left it up to them and just described what we expected to see if we ever went in there.

MR. STEWART: I would say the same.

MR. PAUL STORDAHL: I have a question about what defines PHI. Betty, you mentioned that if you take off the individual identifiers from PHI it's no longer PHI – it's just information. Steele, you said that diagnosis information combined with age and maybe location could give you indications of who an individual is. So which one is safe harbor?

MS. HAYNES: It's actually a little bit of both. The regulation has what they call statistically valid grouping or sample and they went so far as to say if you've got a zip code that has less than 20,000 people in it, as well as if you have people at the defining age of 88, you can't include those types of things even though you've de-identified them because you could find out who the person is. Depending on if it is for the whole country or if it's for a zip code, you may have to tweak it down even more.

MR. STORDAHL: So the regulation does give a safe harbor based upon size?

MR. WOOD: I wouldn't suggest it's a safe harbor.

MS. HAYNES: If you have a report based on having a million members and 100,000 of them have seen a physician in the past year, you're safe. If you say that in Juneau, Alaska you have a 95-year-old who has had a heart transplant, you're not safe because of the smaller zip code area and the age of the person. Even though you've de-identified their name, someone could potentially figure out who the person is.

MR. WOOD: It's really a problem of identifiability. There are rules of thumb in the regulations, but then it really falls back to whether the information would be identifiable. For instance, when you're refunding back to an experience-rated employer. A lot of your plans do this and they say, "here is your claims profile for the last quarter because you know your experience rate is going to depend on it." This is a fully insured group, so you're the corporate entity. They are simply the purchaser. If you give them a claims run-out that gives them the claims profile even by groupings, you may have problems. If the employer only has 500 employees and there are only two people in the $100,000+ category, you've generated identifiable information. It's kind of squishy. It's sort of like the rule of thumb.

MS. HAYNES: It comes down to interpretation because, in the example he just gave, we would provide that information. We will say it's male/female and we do have age bands so we have interpreted that that's something that's necessary in order to be able to work on renewals. When we go out to new groups we expect that the insurer that they currently have is going to give them that kind of summary data so that we can rate them. It is very interpretational. We consider that part of health care operations. There is certain information that we need to disclose in order to be able to renew a group. For the same situation with a group of five you wouldn't get anything.

Chart 1

Compliance Timelines by Regulations

HIPAA Regulation	Final Rule Compliance Date
Transactions and Code Sets	Final Rule released Compliance date: October 16, 2003
National Provider Identifier	TBD
National Employer Identifier	Final Rule released Compliance date: July 30, 2004
National Individual Identifier	On Hold
National Health Plan Identifier	TBD
Privacy	Final Rule released Compliance date: April 14, 2003
Security	Final Rule released Compliance date: April 21, 2005

7

Chart 2

What is Identifiable Health Information?

Health information which contains 1 or more data elements which will allow for identification of the individual to which the health information pertains.

- Name
- Address
- Names or relatives
- Birth Date
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security Numbers
- Medical Record Number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device number
- URL's
- Internet Protocol (IP) address numbers
- Finger or voice prints
- Photographic images
- Any other uniquely identifying number, characteristic or code

10

Chart 3

Examples of Uses & Disclosures

Uses

- Claims Processor reviewing Authorization screen to process hospital claim
- Contract Specialist reviewing Member Claims
- Underwriting running Claims reports on groups
- UM providing clinical opinion to Grievance Manager

Disclosures

- Access to health information via Web or IVR applications
- Verbal disclosures of health information via customer service
- Electronic transmissions of claim/encounter data to external entities
- Providing a report of claims data to the benefit administrator of an ASO group

13

Chart 4

Health Care Operations examples

- Conducting quality assessment and improvement activities
- Evaluating practitioner and provider performance
- Underwriting, premium rating related to the creation, renewal or replacement of a contract for health insurance
- Providing a report of CHF patients to a disease management vendor
- Conducting or arranging medical review, legal services, audit functions including fraud and abuse detection
- Business planning and development, including formulary development and administration
- Business management and general administrative activities

15

Chart 5

HIPAA Regulation Details-Security

- HIPAA regulations define the requirements to preserve and maintain the confidentiality and privacy of electronically stored, maintained or transmitted health information
  - Administrative Safeguards
    - Security Management Process, Assigned Security Responsibility, Workforce Security, Info Access Mgmt, Awareness & Training, Incident Procedures, Contingency Plan, Evaluation, Business Associate Contracts
  - Physical Safeguards
    - Facility Access Controls, Workstation Use, Workstation Security, Device & Media Controls
  - Technical Safeguards
    - Access Control, Audit Controls, Integrity, Person/Entity Authentication, Transmission Security

25

Chart 6

Penalties for Non-Compliance

- **As taken from the federal regulations:**
  - These laws, as well as any standards established under them, supersede any State law that is contrary to them. The Secretary may, for specified reasons, waive this provision.
  - Penalties for failure to comply with transactions and code sets legislation may not be more than $100 per person per violation and not more than $25,000 per person per violation of a single standard for a calendar year.

26

Chart 7

Penalties for Non-Compliance

Penalties for knowing misuse of unique health identifiers and individually identifiable health information:

(1) A fine of not more than $50,000 and/or imprisonment of not more than 1 year;

(2) if misuse is "under false pretenses," a fine of not more than $100,000 and/or imprisonment of not more than 5 years and;

(3) if misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and / or imprisonment of not more than 10 years."

27

Chart 8

Case Study: Inventory of Uses and Disclosures of PHI

Departments / Units that provide health care or treatment	Departments / Units that make payments for health care or treatment similar to a health plan	Departments / Units that bill insurance carriers, Medicare, Medicaid or other third parties	Departments / Units that have access to or generate information related to provision of health care services
▪ Health Services Department Clinic and Fitness for Duty ▪ Health Services (Regional Field Operations) ▪ Employee Assistance ▪ HSD ▪ Health Services (Health Promotion) ▪ Health Services (Occupational Health Nurse Program)	▪ Health Services Department Clinic and Fitness for Duty ▪ Health Services (Regional Field Operations) ▪ Payroll ▪ Risk Management / Claims ▪ HR Benefits ▪ HSD ▪ Health Services (Health Promotion) ▪ Accounting	▪ Employee Assistance	▪ Information Technologies ▪ Alertness Management ▪ Health Services Department Clinic and Fitness for Duty ▪ HR Service Center ▪ Health Services (Regional Field Operations) ▪ HR – EEO ▪ Random Drug Testing (RDT), LEL, EQMS ▪ Risk Management / Claims ▪ Employee Assistance ▪ Supply-Contract Services ▪ HR Benefits ▪ HSD ▪ Health Services, Central Operations ▪ Health Services (Occupational Health Nurse Program)

NYO 10

Chart 9

Case Study: Inventory of Uses and Disclosures of PHI

- On average each Department / Unit has access to 3.3 different programs

Type of Program	Departments with access to Program
Employee Assistance Program	7
Health Promotions	7
Employee Physicals	7
Work Hardening	4
Short Term Disability	5
Long Term Disability	6
Worker's Compensation	3
Wellness	6
Employee Drug Screenings	6
Hearing Conservation	5
Other	6

NYO 11

Chart 10

Case Study: Inventory of Uses and Disclosures of PHI

Sources of PHI	Modes of Communication										
	FAX	Letter	Mail	E-mail	Report	CD	Diskette	File/ FTP	Phone	Face to face	Other (Specify)
Individual	7	10	10	7	9	0	1	3	12	11	1
Contractor	5	6	6	6	6	0	1	3	7	7	1
Physician/ Hospital/ Other Health Care provider	7	7	6	4	6	0	0	1	7	3	1
Health Plan	5	4	5	5	4	0	2	3	5	2	1
Your firm/ organization	8	6	7	7	6	0	1	4	9	7	1
Consultants (e.g. lawyers, accountants, actuaries)	6	6	5	6	5	0	1	2	6	4	1
Third Party Administrator (TPA)	4	4	3	7	7	1	3	3	5	2	0
Other Government Agencies	3	4	2	2	2	0	0	1	3	1	1
Federal	1	1	1	1	0	0	0	0	1	0	0
State	1	1	1	1	0	0	0	0	1	0	0
Local	2	2	1	2	0	0	0	0	1	0	0
County											
Union	2	2	3	2	0	0	0	0	3	3	1
Marketer	0	0	0	0	0	0	0	0	0	0	0
Durable Medical Equipment (DME) Vendor	0	0	0	0	0	0	0	0	0	0	1
Other Vendor	0	0	0	0	0	0	0	1	1	0	0
Other	0	0	0	0	0	0	0	0	0	0	0

NYO 12

Chart 11

Case Study: Inventory of Uses and Disclosures of PHI

Disclosures of PHI	Modes of Communication										
	FAX	Letter	Mail	E-mail	Report	CD	Diskette	File/ FTP	Phone	Face to face	Other (Specify)
Individual	5	5	6	4	2	0	0	1	6	5	0
Contractor	3	2	3	3	2	0	0	1	5	3	1
Family Members	3	3	3	2	0	0	0	0	4	1	0
Physician/ Hospital/ Other Health Care provider	6	6	5	4	1	0	0	0	6	2	1
Health Plan	5	4	5	4	3	0	1	3	5	2	1
Your firm/ organization	5	4	5	4	4	0	0	2	6	4	1
Consultants (e.g. lawyers, accountants, actuaries)	5	5	5	4	4	0	2	2	6	3	1
Third Party Administrator (TPA)	4	5	4	2	3	0	1	2	4	2	1
Other Government Agencies											
Federal	3	4	3	1	1	0	0	0	2	1	0
State	2	3	1	1	1	0	0	0	2	0	0
Local	2	3	1	1	1	0	0	0	2	0	0
County	2	3	1	1	1	0	0	0	2	0	0
Union	1	1	1	0	1	0	0	0	1	1	0
Marketer	0	0	0	0	0	0	0	0	0	0	0
Durable Medical Equipment (DME) Vendor	0	0	0	0	0	0	0	0	0	0	1
Other Vendor	1	1	1	1	1	0	0	1	1	1	0
Other	0	0	0	0	0	0	0	0	0	0	0

NYO 13