Summary of the general question and answer session – Rebekah Pinick, OCR
July 16, 2003 Nebraska SNIP meeting

Question: Our community continues to read the list of admissions and discharges on a local radio station. Can we continue this practice?

Response: If it is in your privacy notice that your directory is posted on the radio, and you give the patient an opportunity to opt out, it's okay.

Q: What are the options for students who may be at another facility as part of their education?

R: If you consider them 'workforce' the responsibility for complying with the requirements of HIPAA (education, actions committed by the students, etc.) fall to the facility that accepts the student. If you treat them as 'business associates', it is the responsibility of the school to provide the HIPAA related education, etc.

Q: How should we handle students who shadow health care professionals?

R: Students would be considered volunteers, which have the same requirements as workforce. Or, you can get a patient authorization for the student to observe the medical care.

Q: How should we handle personal representatives and requests made over the telephone?

R: If you have a copy of the form designating them as the personal representative, it's okay to give out the information. Family members can receive information, subject to the minimum necessary rule.

Q: From an insurance perspective, a family member calls and asks whether the claim is paid. There has been no designation as a personal representative. Can we give out this information?

R: You can disclose for treatment, payment and health care operations without an authorization, subject to the minimum necessary rule.

Releasing medical information is different than releasing payment information. Family members can receive information based on reasonable implied consent, subject to the minimum necessary rule. For example, drug use instructions on discharge.

Regarding personal representatives, put the burden of proof on the personal representative to prove their status.

Q: How should we handle a minor who is a ward of the state? What documentation should we require?

R: A copy of the court order is good. Work with the State to give the foster parent the authority. The State is the legal authority for the minor. It would be acceptable if the State would provide an authorization to release information to the foster parent.

Q: What is the employer's responsibility if insurance is offered via a cafeteria plan. Can the employer keep medical information in the personnel file?

R: If the employer is not a covered entity, the employment records are excepted under the HIPAA rule. If they are a self insured plan, they would be a covered entity so would have to follow HIPAA.

Q: If a provider of health care is not doing electronic transactions now, when do I need to be compliant with HIPAA?

R: As soon as you begin to submit electronically. As of 10/16, Medicare claims must be submitted electronically unless you have 10 or fewer employees.

Q: Regarding military facilities, what are the rights of military members?

R: We are working with the OCR to develop guidance in this area.

Q: We sent a business associate agreement to a vendor but they refuse to sign and send it back. What should we do?

R: This is a contractual issue.

Q: What if we are coerced into signing an authorization?

R: File a complaint with the OCR, or work through the entity for resolution.

Q: I work at an agency for the developmentally disabled. Sometimes a client "goes missing". Can we continue to provide a photo and pertinent medical information to the police?

R: You can continue to provide a photo, and continue to provide necessary medical information to the police. I will try to identify the section of statute for you.

Q: We receive a check/remittance form from Medicare that doesn't belong to us. What should we do? Is that a disclosure that should be tracked?

R: Talk with Medicare/CMS/FI about the issue; can file a complaint if it's an ongoing problem. Ms. Pinick will research to determine if it needs to be included in the accounting of disclosures.

Q: GLB doesn't allow you to release information to a spouse. HIPAA says it's okay. If released, does it need to be tracked in the accounting of disclosures?

R: Under HIPAA, you do not need to track disclosures for TPO.

Q: JCAHO has incorporated some HIPAA requirements into their standards. Have they been working with you?

R: Not me directly, but I assume at a higher level there have been communications.

Q: What is the most common complaint you've received?

R: Incidental disclosures. It's okay to have sign in logs, census sheets.

Q: Regarding the determination of a small health plan, does the $5 million apply to each insurance line separately, or to all the lines of insurance together?

R: I will take that back to the OCR for an answer.

Q: When we are looking for a place to transfer a patient to, we fax information to several facilities, even though we may know that the facility is not going to accept the patient. Should this practice continue?

R: It's okay, although I don't recommend batch faxing in general. But the information should be faxed to facilities that are appropriate to the needs of the person you are requesting placement for (limit by category).

Q: At our hospital, the patient's medical record is stored outside the patient's room. What would the OCR expect to see as 'reasonable safeguards'?

R: The published guidance was addressing this issue in a physician's office, and may not be feasible in the hospital setting. Patient names on the door are okay if for treatment purposes. Document the benefits of this practice to treatment vs. risk of incidental disclosure. If you have someone who is deliberately looking at charts, you may have to rethink your policy. We would look at the hospital's analysis of why they thought it was beneficial. Multiple complaints might cause us to view it differently.

Q: We received an authorization from an attorney's office that is a photocopy and it's obvious that the date was filled in later. What should we do?

R: If it's obvious, send it back.

Q: Some have returned authorizations because their name isn't specified. The name doesn't have to be specified, does it?

R: We don’t require it as long as the person would reasonable know who will receive the information. It just has to be specific enough to identify intent.

The following are the questions and comments that were posted to the NESNIP Privacy listserv prior to the July 16, 2003 meeting. I have added the comments made by Rebekah Pinick, Office of Civil Rights, in a larger, bold type.

Q&A NE SNIP MEETING – 16 July 2003

Q: Don't know if this is a question for the OCR but all the rural hospitals I know are still struggling with how to put together our compilation of costs for our per page charge to the patient. Is there any way that this could be addressed at the meeting on the 16th? Nobody is clear on how to do this. Any help you could give us would be appreciated.

COMMENT: Our process has been to calculate the time an employee spends (hourly salary plus benefits), cost of paper, toner, equipment, overhead, broken out to a per page amount. If you do this once and then apply a Consumer Price Index increase each year, you should be O.K.

R Pinick: Agree with the comment.

Q: Do Business Associate Agreements have to be signed on an annual basis if there is not a contract or written agreement between the two parties? I realize some vendors have contracts which may expire and then with new vendors that have agreements or contracts the HIPAA language must be present, and if not, we have them sign a BA Agreement.

COMMENT: These stand-alone BAs should be treated like any other contract. You can set it up with a two or three year term to avoid the administrative nuisance of annual renewal. The other alternative is to use an "evergreen" format that is a one-year contract with an automatic renewal clause. I prefer at least a two-year term so that you review the agreement periodically. If you have a 60-day notice of cancellation by either party for any reason, the term is not a major factor. We may get additional interpretation about BAs from OCR over time that will eliminate the need for some of these contracts.

R Pinick: Agree with the comment

Q: How about the issue of who can authorize use/disclosure of deceased patient's PHI when there is/will be no personal representative of the estate appointed? In many cases, no PR is appointed due to small size of the estate (i.e. no money) and many states (including NE) have specific procedures for handling small estates that do not require appointment of PR. Must we force people to open estate simply for the purpose of authorizing use/disclosure of deceased patient's PHI???????

R Pinick: At this time, we defer to the state's definition of a personal representative. Watch the FAQ for more information. The personal representative does not have to be appointed by the Court. How ever you determined it before HIPAA would be acceptable.

COMMENT: If no personal representative is appointed, then whomever wants access to the PHI may have to obtain a court order. We follow this procedure for relatives who are just curious. Usually they indicate they are conducting some genealogy research.

COMMENT: Isn't there guidance that states that if the records are requested for treatment of another family member they may be released? For example if a deceased parent had a genetic disease, the

physician treating the son/daughter may request the records for their treatment. What about next of kin? Many practices run under the assumption that the spouse/parent/adult child has right to information as next of kin...

COMMENT: This is exactly what needs clarification!! Under what circumstances must we require court order??? Remember - court orders don't come free!!

COMMENT: The one aspect of the OCR guidance from 12/3/2002 that helps is their 1st Q & A regarding Personal Representatives and a health care power of attorney. They state on p. 33 the clear intent not to change or interfere with existing state law and current practice regarding the designation of personal representatives. Mary's reference is also correct - p. 34 of the Q & A says that if the disclosure is for purposes of treating another individual, you can disclose PHI of deceased individual without authorization. The final reference I'll cite for you is on p. 36 – OCR states that "state or other law determines who is authorized to act on an individual's behalf, this the Privacy Rule does not address how personal representatives should be identified".

COMMENT: According to the "Legal Guide for Health Data" prepared by the Nebraska Health Information Management Association, dated 1999, chapter 3, page 15

> "Deceased patients:
> I) Personal Representatives: the personal representative in the form of an executor or administrator is the appropriate person to authorize release of information. A copy of the court documents stating the personal representtive of the estate should be obtained before fulfilling the request for release of information.
>
> II) Spouse: Where no personal representative has been appointed, the spouse may authorize release of information.
>
> III) Next of Kin: If there is no personal representative and no spouse the next of kin the order set out (adult child, parents, adult sibling, grandparent, aunts or uncles) may authorize the release of medical information.
>
> If state law still determines this, then all of the above still applies, doesn't it?

COMMENT: I wouldn't think a court order would be necessary for a husband or wife, son or daughter of the deceased would have to have a court order. In addition, wouldn't the surviving legal next of kin have the right to the information, no matter what the reason? If they can sign the authorization, then even if they were just curious, that would be fine. Often grieving families do not know what they are looking for. Usually they just want to understand what happened (at least from my experience).

COMMENT: I work for a state government facility and our policy states that we can only release PHI to the personal representative (they must show proof of this designation); otherwise we require the requestor to obtain a court order. Our stringent policy has to do with the nature of our records (psychiatric & substance abuse information).

COMMENT: I agree - but I'd like OCR to bless this!! Some hospitals, etc are taking the position that a PR MUST be appointed or they won't release anything. That seems unreasonable.

COMMENT: My understanding from the presentation we had at one of our SNIP privacy meetings (I think Kelly Clarke gave it) is that the HIPAA regulations have been established for the privacy rights of decedents. That means that only the executor of the estate/personal representative has the right to have

access to the records to prevent other family members from satisfying their curiosity. They stated a specific example of a mother deciding that she wanted her deceased daughter's records because she "just knew she had an abortion sometime." With an executor of the estate or the personal representative having control of the records, they can establish if other family members have the right to this information. Am I way off?? Please be careful with using the "Legal Guide for Health Data" by NHIMA because we have not updated yet addressing the HIPAA privacy changes.

COMMENT: This sounds like a great question for our July session with the OCR representative because it shows how complex it can get when we try to work with HIPAA Privacy Rules, state law and common sense. I am looking forward to getting a response on many of these thorny "real life" issues. The regulations are based on policy, but need to be tested and challenged in our daily interactions with patients.

COMMENT: I agree that is a good question. Nebraska has a law that is in that general neighborhood that Sara mentions, reprinted in part below. It allows a surviving spouse or someone else to tie up loose ends without actually opening a probate estate. It mostly refers to collecting property like bank accounts or cars that weren't jointly owned, so it doesn't give a real warm and fuzzy feeling for use in these situations.

COMMENT: The PHI pertaining to payment, as opposed to the actual medical record, is probably a close enough fit for payers to cooperate with the family member. But the reference to "chose in action" is a legal term that might be stretched to allow the medical record release. That is something the providers have to struggle with more than us payers. One definition of a chose in action is "a right to possession" of personal things. At any rate, the point is that the legislature endorsed the idea of not requiring probate in small estates.

> **30-24,125 Collection of personal property by affidavit.** (a) Thirty days after the death of a decedent, any person indebted to the decedent or having possession of tangible personal property or an instrument evidencing a debt, obligation, stock, or chose in action belonging to the decedent shall make payment of the indebtedness or deliver the tangible personal property or an instrument evidencing a debt, obligation, stock, or chose in action to a person claiming to be the successor of the decedent upon being presented an affidavit made by or on behalf of the successor stating... [the estate is under $25k, the relationship of the person to the decedent, no estate has been opened, the claiming person is entitled to the property]:

COMMENT: The fact that my question has generated so many comments seems proof that an OCR response would be helpful!!!

COMMENT: Thank you for your input. I know the NHIMA guide isn't updated but I'm speaking of only those cases where a PR hasn't been named. I agree with Sara in that I'd like the OCR's blessing. I also agree with you in that the PR (or legal next of kin for that matter) definitely would have control over the access. Example: if I am the legal next of kin for my parents, where no others are named as PR, I would have control over whether or not my aunt, cousin or uncle would have access to the record. Having said that, in the example you give below, the mom's reason does not seem justified. However, who decides what is a acceptable reason to look at the file? For example, if I worry that my relative received care worthy of a malpractice suit(but no proof), can a hospital decide that form of curosity is unjustified? If the next of kin state they want to review the record for possible disorders that can be heredity or predispose you to a condition, how do you know if they are telling the truth? Are you going to review the file to see if the patient had such a disorder? (Don't anwser- this is just meant as an example)

Just briefly looking at the HIPAA rule it states:

"Deceased individuals: If under applicable law an executor, administrator or other person has authority to act on behalf of the a deceased individual or the individual's estate, a covered entity must treat such person as a personal representative under this subchaper with respect to protected health information relevant to such personal representation."

I read that to mean that if someone has the legal authority to **act** as a personal representative, HIPAA states you must treat them as such. This is a tricky situation for sure! I think making someone get a court order IF no law requires such, could be a burden to that person. Maybe I'm wrong though! :)

COMMENT:
Not sure this adds a lot to your debate, but today's HIPAAlert from Phoenix Health Systems attempts to address your deceased patient issue. See "Number 9" below...
H I P A A L E R T -- Volume 4, Number 4 -- July 2, 2003

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=>Healthcare IT Consulting & Outsourcing<=
NUMBER 9: "Because of HIPAA, I cannot give you copies of your deceased mother-in-law's medical records, even if she is dead. I need her authorization to do so!" (Comment by Medical Records clerk to woman asking for copy of her mother-in-law's medical files.)

OUR RESPONSE: Well, if that doesn't confuse the family member! The matter of obtaining patients' authorization to disclose their PHI is complex and requires a sound understanding of the regulations by staff who must handle such requests. Explanations to those making requests for PHI disclosure can be simplified. In this case, a more appropriate response to the requestor would be to explain that a written authorization from the patient is required for the disclosure of the medical records unless the requestor happens to be the patient's personal representative (which should be defined) or state-prescribed guardian; and the fact that the patient is deceased does not change this legal requirement.

Q: To set the stage for my question, we are a covered entity that provides support to developmentally disabled. To go along with the question re: deceased patients/clients. What if we have video footage or photos of a patient/client we provided support to, and they are now deceased. We would like to re-disclose the photo or video footage to put into a newly created video about the covered entities history? Do we not use the photo or footage because there is no one to authorize the use or disclosure of the deceased patient's/client's PHI? This newly created video would be used for workforce training and possibly donor appeals.

R Pinick: Regarding 'workforce training' it would be allowed as health care operations with the reminder that minimum necessary applies.

Regarding 'donor appeals' or fundraising, I wouldn't do it without an authorization from the individual or the personal representative.

Q: Please give us your thoughts on the efficacy of discussing PHI over the phone, if good faith and professional judgment are used to verify the person calling and the authority to receive the minimum necessary PHI.

R Pinick: To the person themselves, it's okay. To a family member, it depends on your policies and procedures.

Q: If the insurance company sent the reasons for denial to the doctor, rather than the patient, and the patient requests it, are you obligated under HIPAA to provide the information?

R Pinick: Yes.

COMMENT: I've had several people in my department come up to me and ask about what can and can't be released over the phone to people who call in. I'm putting together a presentation for them but would like to know what the general community is doing since we seem to be "Holding our cards very close to our chests" when it comes to releasing info here. How do you make sure that if a "patient" calls that it really is him?

COMMENT: It is very hard to distill all of the disclosure rules to a quick phone reference. The best guidance is still the OCR HIPAA Privacy guidance that was issued on 12/3/2002. Just copy the section on "Uses & Disclosures for Treatment, Payment and Healthcare Operations if you want the basics. It is 10 pages long and covers the most critical areas. If you want to be more thorough, you can add any of the other disclosure sections that apply to the setting (E.g. public health, personal representatives). The entire guidance is a little over 100 pages. If you add tabs for the content chapters it is very quick and easy to use.

COMMENT: In our little department here we don't have a lot of day-to-day activity with phone requests. To verify "in good faith" whom you are speaking to, ask them for their DOB and SS#. We don't give patients any medical information from our office; they are referred to their doctor. Billing information (I don't handle this) I would assume is made available to them.

COMMENT: As a general rule, we don't give out any PHI over the phone. The only reason I can see to do that would be to give information to another provider for emergency care, which can usually be done by fax (and you can verify the fax #). For non-emergency releases we have the patient present to the department, or write in for the information, so we can verify the request is valid.

Maybe I am being too conservative, but how do you really know who is at the other end of the phone? You can make a "good faith" effort to verify, but we have decided that we don't want to take that risk for non-emergency situations.

COMMENT: Thank you, and I agree, I guess I'm looking at it like this: for instance someone is looking for a missing person, would you tell them if they had been admitted last week, etc. I'm just trying to think of all of the off-the-wall things I could be asked by my clerks when I present them this info and what I would say other people are doing.

COMMENT: Even if it was supposed to be a police officer, it would still not be appropriate by phone. You could have an abusive ex-spouse who has DOB & SS# trying to track down an individual who does not want information shared.

COMMENT: There are many ways to verify and validate individuals, not just DOB & SS#. HIPAA does not specifically prohibit discussion of PHI over the phone. As mentioned below, there are many instances where information could and should be discussed over the phone, of course with the understanding between the parties that most conversations are not over secure telephone lines.

To make a wholesale restriction against phone discussions is inappropriate. Good faith verification and professional judgment should guide your decision on a case-by-case basis. For example: the police officer has a badge number and place of duty; you can call the department back using your own telephone book and find out who goes with the badge number.

COMMENT: I agree with Jeff. The only thing we will give over the phone is discharge date to an insurance company if they have patient name and date of admission and we verify insurance coverage in the computer. Other than that, we absolutely give out no information over the phone. In fact we instruct our staff to not even look up the patient's name in the computer until we have a signed authorization in hand. We ask the patient to come into our department or we send them an authorization via fax and then follow ROI procedures, compare signatures, etc. I have no problem telling people over the phone that what they are asking is "... confidential information and we have an obligation to protect that. Therefore, you will need to ....."

The law enforcement issue and emergency treatment, I agree, are different issues, but what the original e-mail questioned was "how do we know if a patient is calling".

COMMENT: I agree. I do not imagine that patients will be very happy if they cannot get any info unless they come in person. I do not believe either the letter or spirit of the privacy regs require such a policy.

Q: We found that it is very costly to dispose of IV bags by shredding. Since the only information on the bag is the patients name and the name of their medication does disposal of IV bags fall within the "incidental disclosure" category?

R Pinick: Look into tear off labels, shredding, incineration, and then decide what is a reasonable safeguard.

Q: In our community, our facility has had the practice where the hospital minister will send a letter to the patient's minister, just telling them that the patient is at the hospital, and that our ministerial services are there to assist. No medical information is included. We do give patients the opportunity to 'opt out' of this service. Can we continue this practice under HIPAA? Do we need to have an authorization, rather than just the 'opt out' option?

R Pinick: Clergy has more flexibility than the media. Include this practice in your Notice of Privacy Practices. For a patient who is unconscious, if consistent with prior instances, it's probably acceptable.

Q: Will you be incorporating HIPAA workforce language into your clinical affiliation agreements, or maintaining the business associate addendum to the agreement? We sent a clinical affiliation agreement with HIPAA workforce language in it to another Hospital for clinical perfusion students. It was returned, with the recommendation that an amendment to the existing agreement be created, adding the specialty to Exhibit #2. The agreement expires Nov 30, 2004. We would prefer having standardized clinical affiliation agreements with workforce language. Thanks.

R Pinick: As discussed in morning session.

COMMENT: We have been avoiding "workforce" language for two reasons - 1.) We do not believe the term "trainee" was meant to include students and on-site faculty who fall outside the definition of "employment"; and 2.) We do not want to acquire any expanded liability from this designation. I will submit a question for the OCR representative who is attending the July NE SNIP meeting asking if affiliation agreements require BAs. Although they indirectly perform functions on our behalf, the purpose is their own training, and they are not acting independently. I would like to see this clarified and avoid the need for BAs on these numerous clinical affiliation agreements.

Q: What is the latest feeling regarding registries? Obtaining patient consent or not? Business as in the past or changes?

R Pinick: For reporting as mandated by the state, no authorization. For other sharing you would need an authorization or an IRB.

COMMENT: If the registry is mandated by law, then no individual authorization is required. Otherwise, obtain individual authorization if PHI is disclosed. Registries maintained for research require an authorization, unless an exception applies, such as IRB waiver of authorization, disclosure of a limited data set; or disclosure of information on decedents.

COMMENT: In addition to Sheila's comments, those registries and databases you contribute to that aren't required by law, but that you contribute to with the intention of receiving back quality improvement information, can be reported to without patient authorization. Your organization just needs to have a written statement on file with your Privacy Official stating that participation in those databases is a part of your quality improvement process, thus a portion of health care Operations, as defined in the HIPAA regulations.

Q: Is it allowed under HPAA to send unencrypted protected health information to members of the workforce via an intranet, i.e. an internal network. Is it correct to state that any protected health information that is sent over unsecured channels like the internet must be encrypted?

R Pinick: Contact CMS.

Q Our software vendor, who has offered to test claims through their system, told us that the new HIPAA guidelines require us to use the SSN's or TIN's of the referring physician, and not their UPIN number. Is this statement correct? If this were the case, we would have to obtain the SSN/TIN of the all the referring physicians in our database. I can predict that getting this information will be very time consuming and difficult because of identity theft fears. UPIN numbers are published numbers by Medicare, but SSN's and TIN's are not. Many providers are going to be reluctant to give those out.

R Pinick: This is a transactions question. Contact CMS.

Q Since HIPAA states it is a floor, not a ceiling, and therefore other state or federal privacy laws that are more protective, will still apply in addition to HIPAA protections, do disclosures that might not require an accounting under HIPAA rules, still have to be accounted for if another privacy law prohibits those disclosures?

R Pinick: Yes. If neither law requires an accounting, you don't have to account for it.

For example, disclosures made to persons involved in the individual's care do not have to be accounted for. Under HIPAA that type of disclosure may be allowed, but under GLB this issue is not addressed, to my knowledge, and disclosure of such information would be prohibited without an authorization. Since HIPAA says that more stringent laws are applicable, are such disclosures technically a violation of HIPAA in a round about way because they violate some other privacy law, and therefore need to be accounted for?

Q: When the regulations discuss disclosures for "work comp or similar programs" in 164.512(l) - does that include FELA (railroad injuries)??

R Pinick: FELA is not among those listed; I will take that back to the OCR for clarification.

Q: To hand out the privacy notice to every patient (>14,000) at our flu clinics is going to be very costly. Does the OIG have any suggestions on how to best handle this situation?

R Pinick: You still have to provide a NPP and post it. There is no stipulation as to font size.

Q: Will the regulations ever be changed to exclude the accounting of disclosures for legal and mandatory reporting. IE: to child protective services, Adult protective services, etc.

R Pinick: At this time you are still required to account for such disclosures.