NBDPN HIPAA Awareness for Birth Defect Surveillance Systems

As of this writing, (June, 2002) the Privacy Rule is undergoing modification. These changes are unlikely to increase the burdens on surveillance systems and, in some cases, may alleviate them. This document will be updated as necessary.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by Congress to implement broad health care reform. Congress then used HIPAA to require passage of comprehensive medical privacy legislation and gave itself 3 years in HIPAA legislation to enact privacy legislation. HIPAA itself does not address privacy except to mandate the establishment of standards. If Congress did not enact legislation as required, then HIPAA required the Secretary of HHS to promulgate the privacy legislation. Congress failed to enact legislation and as a result, HHS issued "Standards for Privacy of Individually Identifiable Health Information" (Privacy Rule).

The HIPAA addresses the right of individuals to have health insurance and protection from healthcare abuse and fraud. It also has a subpart requiring the Department of Health and Human Services to adopt national standards for electronic medical record keeping and transmission. The national standards for electronic transmission of data is in the Security section of the Rule, and has different compliance requirements that are beyond the scope of this document.

The Standards for Privacy of Individually Identifiable Health Information became effective April 14, 2001 and comprises the privacy standards mandated by HIPAA. The Privacy Rule sets minimum responsibility standards for health care providers regarding how information is disseminated and Used. It also enables patients to find out, and limit, how their information is utilized.

HIPAA and its rules apply to personal information in any form. They establish a minimum standard of privacy protection which may be intensified by the state. (This is often true - federal law may be trumped by a stricter state law.) A central issue of HIPAA is electronic transmission of personal medical information and, thus, these transmissions must also conform to the HIPAA privacy standards. In this context "transmission" means something as simple as saving the information on a disk or a hard drive. It does not only mean sharing the information with another person.

The Privacy Rule is a significant burden on health care providers. They are required to enhance and document intramural procedures that maintain confidentiality, ensure that all persons or entities with provider permission to access those records also maintain confidentiality, and educate patients of how their information is used and by whom. Penalty for misuse or broadcast of the information falls to the health care providers, even if they are not the ones who violated the Privacy Rule. Thus, it is understandable that health care providers may become diligent about who has access to information, how that information is gathered, and how it is used by the outside source.

Public health entities are exempt from the HIPAA-related Privacy Rule, and there are provisions for research using patient identifiers. So, most surveillance systems are not covered entities and do not need to meet the Privacy Rule. Those surveillance systems mandated by state law have other legal protections that allow access. However, the health care providers bearing the burden of Privacy Rule are within their rights to ask questions of and have assurances from birth defect surveillance systems.

Most health care providers have until April 2003 to institute the Privacy Rule. Health care providers and plans with less than 500 clients or patients have until April 2004 to comply with the Privacy Rule.) Because of the flexibility allowed, it may be assumed that there will be no single method or process instituted. It may be further assumed that some of the procedures will place a burden on birth defect surveillance systems. This document covers those situations that have already arisen or which are anticipated. Remember that each situation may be unique and these recommendations are to be considered a minimum standard.

A question and answer document about the Privacy Rule can be found at the Office for Civil Rights webpage: http://www.hhs.gov/ocr/hipaa/finalmaster.html There is also information on the CDC website: www.cdc.gov/cic

Background Homework

Know the legislation, statute or other regulation that supports your birth defect surveillance program. Make sure that each member of your staff has this information - both full text and the citation. If the documentation is complex, provide the staff with a summary (with appropriate references). You may want also to supply your supervisory level, legal office and public relations office with this information.

Understand how the federal HIPAA Privacy Rule applies to public health surveillance and research. (See website listed on introduction page.) Further, review whether your state has its own HIPAA Privacy Rule. If your state has provisions, they may be more strict than the Federal rules. You should understand any differences between federal and state privacy rules.

It is best if your staff understands the basics of Federal (and, where applicable, state) HIPAA Privacy Rules. At the minimum, they should learn to recognize when a health care provider policy or request is being driven by the HIPAA Privacy Rule. The Office for Civil Rights has compiled a document answering frequently asked questions about HIPAA Privacy Rule impact on public health entities. It is included in the abstract book from the 5th Annual NBDPN meeting. It can also be found in draft form at: http://www.nahdo.org/memberaccess/fact1.pdf.

Justifying Public Health Access[1]

Health care providers may ask for documentation proving that your abstractors are working for a mandated public health surveillance program. In anticipation, prepare a document on Department of Health or surveillance program letterhead that includes the following (in no particular order). A model for this information may be your state's one-page description as published in the annual *Teratology* compilation:

Title of the program
Program director name, address, contact number
Relevant state legislation citation (or a full copy if possible)
    If your legislation includes confidentiality requirements/provisions, include full documentation of it.
Brief history of your program
Brief definition of your program.
What access you need - be as specific as possible about what you need from the health care provider.

For a particular institution the name, address and contact number of the abstractor and his/her immediate supervisor.

Staff Identification

It is reasonable for health care providers to request identification of individual surveillance staff even if they have the above documentation about the surveillance program. The following may help decrease staff time spent providing information for each contact.

Consider the use of specialized staff identification badges. An extra badge, color coding, or additional stamp or seal that identifies individual staff as being employed by a public health entity with access to HIPAA-regulated materials. This may, for example, indicate that the staff member has signed a confidentiality statement, received specific training about HIPAA and the privacy rule, or other formal acknowledgement of special status to access personalized health information.

At least annually, send all surveyed health care providers a list of staff who may ask for access to personal health information at that provider. An annual mailing would account for any staff turnover and would reinforce the status of continuing staff. Depending upon the needs of the health care provider, it may be necessary to send additional mailings during the year to notify them of any staff changes.

Please note that allowing staff access to medical records does not need to violate the personal privacy of that staff member. If a health care provider requires private information from the staff member (home address, home phone number, social security number, driver's license number, etc) it is reasonable to question the necessity. Staff members should only be expected to volunteer business related data (work address, work number, employee number, supervisor's name, etc.).

Confidentiality Statements

Health Care Providers may request that your surveillance staff sign confidentiality statements from the provider. Educate your staff about this and about whether they may legally sign these documents. At the very least, allow for some sort of document review before the employee signs the statement. Some government employers (particularly federal government) do not allow their employees to sign such documents.
It is possible that such documents might put the employee in an indefensible or conflicted position. For example, the confidentiality statement may insist that identifiable patient information may not be entered into a database searchable by those who have not signed the statement. Or, it may require that the Provider be notified any time the information is accessed out of the surveillance database. Obviously, these would be impossible for the surveillance employee to sign: the requirements of the Provider's confidentiality statement are either in conflict with the surveillance system work or simply too laborious to complete.

Consider establishing, if it doesn't already exist, a division-wide or department-wide confidentiality statement for all your employees. Provide each employee with a copy of their own signed (perhaps notarized) statement which they can share with health care providers. This statement should be considered to supersede any health care provider statement.

Privacy Officer

Health care providers will designate a "privacy officer". This may be an office manager with other duties, or may be someone hired specifically to oversee HIPAA Privacy Rule enforcement. Find out who this person is, all their contact numbers, etc. It is important also to know how to contact them outside of regular business hours (pager? cell phone number?) and who is their proxy when they are unavailable.

Additionally, it will be helpful for someone in your surveillance main office to be designated as a "privacy officer". This person would be made responsible for knowing the HIPAA and Privacy Rule language, relevant dates, statutory changes, etc. for both federal and specific state HIPAA. In addition to being an information source for other staff, this person could field questions from health care providers. Having a single, specific contact for questions is likely to be an asset.

Institutional Review Boards and Legal Offices

Health care providers may involve their Institutional Review Board, Ethics Committee or Risk Management Office in enforcement of HIPAA Privacy Rules. Hopefully this will diminish as comfort increases. The most significant difficulty in this situation is the delay imposed by committee or legal review.

If told that there will be IRB, Ethics or Risk Management Review, the following is suggested:

• Find out the name of the IRB chair, Ethics committee chair or risk management officer and their contact number. Deal directly with this one person if you can.

• Ask about their standard method of expediting review. It may be possible to speed or bypass review by a large committee.

• Ask when/where the committee review will take place and plan to be there. Don't ask for permission to appear, tell them you will be there. That will give you a chance to present all your supporting documentation yourself, rather than relying on someone from within the hospital to present your case. This should be within the standard operating procedure of the committee: when there are patient cases it is typical that the Ethics Committee hear from the patient, doctor, and any one else involved, so there is easily precedent for "outsiders" to present their case.

• Require a deadline. Find out precisely when you can expect resolution of the question and be clear about what you expect.

Requirements for Researchers

Your surveillance system should already have in place regulations covering release of identifying information for research. In addition to your own standards, researchers should be aware of HIPAA rules pertaining to use of identifiers in research. Health care providers may reasonably require any researcher requesting identifying information to submit the research protocol also to the health care provider if the information comes primarily from that health care provider's records.

Someone in each surveillance system should review HIPAA Privacy rule content regarding research. Be prepared to amend language in any relevant intramural documents. It may also be necessary to amend your legislative mandate to address HIPAA Privacy rule requirements. Particularly, understand when the surveillance program must involve the health care provider in a research protocol.

Consider obtaining, requiring or recommending a Certification of Confidentiality for research done with surveillance data.

Enforcement of Birth Defect Surveillance Legislation

Your own state legislation mandating birth defect surveillance may provide you with recourse when denied access. Though it should be seen as a last resort, health care providers should be made aware that they are violating existing state law by denying you access to medical records. Certainly it is better not to be (or be seen to be) belligerent, but you do have existing law on your side and can make that clear.

Understand who is responsible for reinforcing your mandate. It may be the state legislature, Commissioner of Health or the state attorney general. It may benefit you to be in contact with the state congress person responsible for the region in which a particular health care provider resides. If you have persistent problems, you may wish to inform the state attorney general's office. It may also be helpful to notify the Centers for Disease Control and Prevention National Center on Birth Defects and Disabilities that your surveillance system is having difficulty obtaining access.

State Surveillance Legislative Mandates

If your birth defects surveillance system is not covered by state legislative mandate, consider establishing it. This will provide your system with an enforceable right to access personal medical information that may be restricted by health care providers. There are examples of state legislation available.

Exempting Health Care Provider from Liability

Consider establishing state law that would excuse health care providers from liability based on use and misuse of confidential information by state surveillance programs. In practice, this would probably be an unnecessary law; however, it may provide a modicum of comfort to health care providers. Such legislation would potentially place a burden on the surveillance system, so it is important for the surveillance system administration to be involved in the formation of any law. Also, the process of considering such legislation may point out areas within the surveillance system that are confidentiality problems.

1 The health care provider may require verification as described in paragraph §164.514(h)(2) of the rule. This includes:

> "(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
>
> > (A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
> >
> > (B) If the request is in writing, the request is on the appropriate government letterhead; or
> >
> > (C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
>
> (iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
>
> (A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
>
> (B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority." (See §164.514(h), 65 F. R. p. 82820 for complete requirements.)