HIPAA Privacy Considerations for Community Access Program Grantees

Prepared for the Health Resources and Services Administration

by:

Powell, Goldstein, Frazer & Murphy, LLP

with the assistance of

Feldesman, Tucker, Leifer, Fidell & Bank, LLP

March 1, 2001

* * * * *

Note: These materials were prepared just as a new comment period was opened for these regulations. Comments are due March 30, 2001. There may be subsequent changes to the regulations as a result of the new notice and comment process.

This document has been prepared for HRSA under by the law firms listed above. The U.S. Department of Health and Human Services has not verified the accuracy of data or analysis presented in the document. The opinions expressed in this document are the views of the authors and do not necessarily reflect the official position of the Health Resources and Services Administration or the Department of Health and Human Services.
This document is designed to provide accurate and authoritative information in regard to the subject matter covered. It is issued with the understanding that the authors are not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

HIPAA Privacy Considerations
for Community Access Program Grantees

I. INTRODUCTION

The "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") directed the Department of Health and Human Services (DHHS) to take several important steps towards increasing efficiency in the health care system. Congress directed DHHS to work with the industry to adopt or develop standards for certain electronic health care transactions (*e.g.*, claims and claim status, health plan enrollment and eligibility, and referral certification and authorization). DHHS was also charged with developing certain uniform code sets (*e.g.*, diagnoses and procedures) and several different identifiers (*e.g.*, health plans, employers and providers).[1]

Recognizing that health information would be flowing much more freely once these transactions, code sets and identifiers were all standardized, Congress also directed DHHS to develop regulations governing the security and the privacy of health information. In August of 1998, DHHS published a proposed security regulation that requires covered entities to have physical, technical and administrative safeguards in place – such as access controls (*e.g.*, passwords), disaster recovery plans, and data and entity authentication systems. DHHS is still in the process of finalizing this regulation.

The privacy regulation was proposed in November 1999 and was published in final form in the last days of the Clinton Administration. The regulation included sweeping protections for individually identifiable health information and provided patients with a host of new individual rights. Most of the industry is currently expected to come into compliance by April 2003, but the Bush Administration has re-opened the regulation for comment until March 30, 2001 and is considering policy changes.

This issue brief is intended to provide an overview of the privacy regulation and offer some insight as to how the regulation may specifically impact grantees and CAP network participants ("participants") under the Community Access Program (CAP). While participants and CAP grantees are not expected to be in compliance immediately, they are in the position of developing new systems that will be used for many years to come. Grantees should understand the expectations at the federal level and build in the capacity now to ensure that these systems will be able to come into compliance when necessary.

---

[1] A few of these regulations have been published in proposed form, but only one – the regulation governing electronic health care transactions – has been published in final form. See http://aspe.hhs.gov/admnsimp/Index.htm. This website is a good resource for keeping current with HIPAA developments.

II. SUMMARY OF THE HIPAA PRIVACY REGULATION

For three classes of entities, the regulation establishes a new framework that will govern all uses and disclosures of certain patient information. In addition, the regulation is intended to empower patients to understand and control their information by creating several new individual rights. If a covered entity does not comply with the requirements of this HIPAA regulation or any one of the other HIPAA regulations, it could be subject to both civil and criminal penalties.

A. Who Is Covered by the Regulation?

Due to limitations in the statutory authority under HIPAA, only certain entities fall within the scope of the privacy rule. The regulation applies to three categories of "covered entities": health plans (including State Medicaid and SCHIP agencies), health care clearinghouses and health care providers who transmit health information in electronic form in connection with certain transactions. The regulation, for example, does not apply to a county agency that does not provide any health care services. It also does not apply to a provider who does not engage in any electronic health care transactions. It is important to note that if a provider does not conduct these transactions on site, but rather contracts with a billing agent to conduct them for the provider, the provider would still be considered a covered entity. It also is important to note that once a provider is covered, i.e., by transmitting health information in electronic form, the provider is subject to the privacy regulation for all types of health information, including written (paper), oral and electronic.

In some instances, the requirements of the regulation will extend to other entities that are working with a covered entity. These entities are called "business associates." An entity is a business associate if it performs a function on behalf of the covered entity involving the use or disclosure of individually identifiable health information, such as a billing company. An entity is also a business associate if it has access to individually identifiable health information from a covered entity or another business associate of a covered entity in order to perform specific services, including legal, actuarial, accounting, consulting, management, administrative, accreditation, data aggregation and financial services. In these situations, the covered entity will have to enter into a contract which requires the business associate to take certain steps to protect the privacy of the information it receives. The covered entity will be held responsible for any inappropriate disclosures by the business associate (unless the business associate is also a covered entity).

The first part of the definition of business associate is somewhat ambiguous: When will an entity be performing an function *on behalf of* another entity as opposed to simply performing the function independently? For example, consider an organization that operates a nurse consultation line that provides general advice to consumers and may refer an individual to a local provider if care is needed. Does the organization become a business associate of the provider? If the hotline organization is simply maintaining a list of all providers in the area and providing referrals to individuals that call, it is probably not a business associate and therefore no contract would be required. If, however, the organization and the provider share a central information system and the hotline representative enters information into the system for the provider to use when she treats the patient, has the organization become a business associate? Possibly. In this case, the provider should consider entering into a business associate contract with the

organization. Expanding this example to include all of the different providers in the CAP network, in order to reduce the administrative burden, the CAP providers should consider developing standard contract language for this particular relationship.

B. What Information Is Covered by the Regulation?

The regulation applies only to "protected health information" (PHI) which is defined broadly to mean individually identifiable health information transmitted or maintained in any form or medium, including written, electronic, and oral forms. "Individually identifiable health information" is information, including demographic information, that identifies the individual or with respect to which there is a reasonable basis to believe that the information could be used to identify the individual and relates to the individual's past, present or future health condition or payment for health care.

If information is de-identified, it is not covered by the regulation – but it is extremely difficult to achieve de-identification. The entity must either strip all identifiers (*e.g.*, name, Social Security number, record numbers, account numbers, demographic information, serial numbers) or else it must have a person with statistical expertise configure the information in such a way that the expert is satisfied that the information could not be re-identified. The regulation outlines several specific requirements that apply if the entity elects to assign a code to de-identified information that allows it to be re-identified.

Many CAP grantees are planning to coordinate care for uninsured individuals receiving care from different providers in the community. In most instances, the providers will need to share identifiable information and therefore those activities would fall within the scope of the regulation. Grantees should evaluate their planned activities to determine if any can be conducted with de-identified information instead. For example, if a grantee is planning to develop a quality improvement system, the system could be designed to only use de-identified information. However, given the difficulty of de-identifying data, grantees may want to weigh the costs of de-identification compared to getting authorizations.

C. When May Covered Entities Use and Disclose PHI?

Covered entities may only use and disclose PHI in a manner that is either permitted or required by the regulation. The regulation only requires disclosure in two instances: when the individual requests the information, and when DHHS requests the information to investigate the entity's compliance with the regulation. An entity is *permitted* to use or disclose PHI only if it has the individual's permission or if the regulation specifically permits the use or disclosure without the individual's permission.

1. Individual Permission

The regulation includes four different concepts regarding obtaining an individual's direct or indirect permission: (a) consent, (b) authorization, (c) an opportunity to agree or object, and (d) an opportunity to opt out.

(a) Consent

Health care providers are required to obtain an individual's consent to use or disclose PHI for treatment, payment or health care operations, even for uses within the same institution. Before addressing the specific requirements for a consent, these terms – treatment, payment and health care operations – should be explored in more detail.

Under the regulation, treatment means the provision, coordination or management of health care and related services by one or more health care providers. This includes consultation between health care providers relating to a patient or the referral of a patient from one provider to another. Treatment only applies to care for an individual, not for a population. A provider is allowed to condition treatment on the provision by the individual of a consent.

Payment is defined to include activities by health care providers or health plans to obtain or provide reimbursement for the provision of health care. The regulation identifies a non-exclusive list of activities that are considered payment, including determinations of eligibility or coverage, billing and collection activities, medical necessity reviews and utilization reviews. In evaluating CAP grants, the Health Resources and Services Administration (HRSA) emphasizes the importance of establishing links with social service programs and public benefits programs. Several grantees are planning to use CAP funding to create systems for providers to have access to information about all public benefit programs and to determine eligibility. In most instances, these activities would fall within the definition of payment.

The category of "health care operations" encompasses a wide range of activities that covered entities must engage in to remain viable. Some of the activities that fall within this category are:

- Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines (provided that the activity is not primarily intended as research to contribute to generalizable knowledge);

- Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives, and related functions that do not entail direct patient care;

- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs, accreditation, certification, licensing or credentialing activities;

- Conducting or arranging for medical review, legal services and auditing functions (including fraud and abuse detection and compliance programs); and

- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary

development and administration, development or improvement of methods of payment or coverage policies.

In part, CAP is encouraging communities to focus on these types of activities and search for innovative ways to integrate them in order to improve the quality and coordination of care for the uninsured population. For example, many grantee networks are collaborating to develop centralized disease management and case management systems. If an individual provider is doing these types of programs for individuals, it is likely that they would fall under health care operations. It is a much more complicated question if multiple entities are sharing information while creating these systems together. Section 2 below focuses on how multiple covered entities will be able to comply with the regulation while engaging in the type of information sharing necessary to integrate these health care operations.

For these three categories of activities – treatment, payment and health care operations – providers are generally required to obtain a consent. Health plans and clearinghouses are permitted to obtain a consent for these activities, but they are not required to do so. There are certain circumstances where a provider is not required to obtain a consent, including:

- If the provider has an indirect treatment relationship with the individual (*e.g.*, a radiologist or pathologist);
- If the provider has difficulty communicating with the individual, but the consent can be inferred;
- If it is an emergency treatment situation; and
- If the provider is required by law to treat the individual.

This last exception is particularly significant for many public providers and community health centers participating in CAP because they are often required by state law or as a condition of receiving grant funding to provide care for the uninsured. If an uninsured patient is seeking treatment at a health center but refuses to sign a consent to the center's use or disclosure of PHI, the center may fall within this exception and therefore would be able to use and disclose the information for treatment, payment and health care operations.

The regulation specifies the type of information that must be included in a consent in order for it to be valid. Notably, a consent is *not* required to include an expiration date, but the individual may revoke the consent at any time.

(b) Authorization

An individual authorization is an entirely different document than a consent and has separate rules that apply. An authorization is required for any use or disclosure that is not permitted by any other part of the regulation. It is different from a consent in several important ways:

- In most instances, the entity may not condition treatment or payment on the individual signing the authorization.

- An authorization must include several specific elements that are not included in a consent – one of which is an expiration date or event.

- Special rules apply depending on whether the entity requests the authorization for its own uses and disclosures or for those by another entity.

(c) Other Permissions

The regulation identifies two other categories of individual permission, but these categories are extremely limited in scope and the requirements are far less cumbersome. First, an entity must provide the individual with an opportunity to agree or object to disclosures from facility directories (*e.g.*, hospital patient information lines) or disclosures to other people who are involved in the individual's care (*e.g.*, family or friends). Unlike the consents and authorizations, the individual's agreement or objection may be verbal. Second, an entity must provide the individual with an opportunity to opt out of certain uses and disclosures for either fundraising purposes or marketing. For example, if an entity sends marketing materials to an individual, the materials must explain how the individual may opt out of receiving such materials in the future.

2. Uses and Disclosures Allowed Without Individual Permission

An entity may use or disclose PHI without the individual's permission only under the specific circumstances outlined in the regulation. The circumstances are intended to encompass those activities that are national priorities such as law enforcement activities, judicial proceedings, public health activities, health research and when necessary to avert a serious threat to health or safety.

One of the circumstances identified in the regulation involves disclosure to certain government programs providing public benefits. In limited circumstances, government agencies and programs will be able to disclose information without the individual's permission. Specifically, the regulation allows:

- A government program that is a health plan (such as Medicaid or SCHIP) may disclose PHI relating to eligibility or enrollment to another agency administering public benefits if the sharing of the information (or maintenance of the information in a shared database) is required or expressly authorized by statute or regulation.

- A government agency that administers a public benefit program may disclose PHI to another government agency that administers a public benefit program if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate or improve the health care functions of the program.

In order to expand outreach and increase enrollment in public programs, many CAP grantees have included government agencies, such as the Medicaid and/or SCHIP agencies, in their grant.

This provision of the regulation will allow the State or local agency to play an important role in the grantee's outreach efforts. For example, a provider may submit patient information into a centralized Medicaid eligibility system in order to determine whether it can receive payment for the services it rendered. Once the Medicaid agency has this information, it would be in a position to share it with other programs that serve the same population (*e.g.*, WIC, Head Start) without the individual's permission.

D. How Much Information May Be Used and Disclosed?

In general, when using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary requirement does not apply to certain types of disclosures, including disclosures to or requests by a health care provider in connection with treatment, disclosures made to the individual, most disclosure made pursuant to an authorization and disclosures that are required by law.

In order ensure that the covered entity only discloses the minimum information necessary, the entity must have policies and procedures for handling routine disclosures and non-routine disclosures, as well as criteria for evaluating how much information should be disclosed. In order to comply with the minimum necessary use requirement, each entity must limit access to PHI to only those people within the organization who need access to the information to carry out their duties. In addition, access by those people must be reasonably restricted to the information necessary to perform their functions.

For CAP grantee networks, this "minimum necessary" standard will require each participating organization to evaluate its own need for information and will also require any centralized systems to examine how access to information will be limited to comply with this standard. For example, if the grantee network is developing a shared information system for participating providers, the system will need to evaluate for what purpose the information being sought (if for treatment, broader access is permitted; if for payment, the scope needs to be restricted), and discriminate among the type of people accessing the information (it could be reasonable for a doctor to have access to the entire medical record; a physical therapist may not need information on sexually transmitted diseases).

E. What New Individual Rights Are Established?

The regulation establishes numerous new individual rights that are intended to empower individuals to understand and control how their health information is used and shared. The rights established in the rule include: the right to request restrictions on release of PHI, the right to request confidential communications, the right to a notice of privacy practices, the right of access to PHI, the right to have PHI amended and the right to receive an accounting of disclosures. Many CAP grantees and participants will need to evaluate how they will implement these individual rights both as independent covered entities and also collectively as a network.

1. Right to Request Restrictions on Uses and Disclosures

A covered entity must permit an individual to request that the entity restrict uses or disclosures of PHI in carrying out treatment, payment, or health care operations. For example, an individual may request that a provider not use his health information in developing treatment protocols. The individual must also be able to place restrictions on when the entity shares information with others involved in the individual's care, such as family members or friends. The covered entity is not required to agree to any of these restrictions. However, if the entity does agree, it must document the restriction and it must not use or disclose PHI in violation of such restriction except in certain emergency treatment situations. Certain types of disclosures would not be affected by such a restriction (such as disclosures for law enforcement, research and public health).

This provision presents CAP grantee networks that use a shared medical record system with a significant administrative challenge. The regulation is clear that a restriction is only binding on the entity that agreed to it – but it is not clear how information should be handled if several entities share an integrated medical record system. For example, if one provider accepts such a restriction and then submits the patient information (including the restriction) into the centralized system, will the system be programmed to prevent disclosures of the restricted information by that one provider or will it extend to all users of the system? When possible, providers might wish to negotiate among themselves uniform approaches on accepting restrictions. Grantees should also require participants to notify patients that one provider agreeing to restrictions does not automatically bind all the other providers. Grantee networks using these types of integrated systems should evaluate their system's capabilities individually and explore whether changes are necessary.

2. Right to Request Confidential Communications

An individual has the right to make special requests that covered providers and plans communicate with him or her in particular ways to preserve the confidentiality of the information ("confidential communications"). Under some circumstances, providers and plans are required to accommodate such requests. For example, an individual who does not want his or her household members to know about a certain treatment may request that the provider communicate with the individual at work. As with the agreed-upon restrictions discussed above, these requests present operational and technical challenges for different entities that share integrated information systems and participate in coordinated systems of care.

3. Right to Receive a Notice of Privacy Practices

Except in limited circumstances, an individual has a right to an adequate notice that describes the entity's uses and disclosures of PHI, the individual's rights with respect to PHI maintained by the entity and the entity's legal duties with respect to that PHI. This notice requirement is extraordinarily detailed; it is likely that each entity's notice will be several pages in length. It is critical that each entity prepare an accurate and complete notice because, under

the regulation, it will be bound by the statements in the notice. In other words, the entity may not use or disclose PHI in a manner that is inconsistent with the notice.

The regulation specifies how and when the notice must be initially disseminated and also what steps the entity must take if it revises the notice. If several entities are involved in an "organized health care arrangement," they may be able to use a joint notice. (See Section 2 below for a more detailed discussion of organized health care arrangements.)

One of the challenges for covered entities participating in CAP programs will be explaining *in plain language* exactly how they will be using and disclosing PHI, and obtaining the necessary consents and authorizations. Many grantee networks are planning to implement complex systems of information sharing and coordination that may be difficult to explain to the average patient. For example, patients could easily become alarmed by a notice that explains that all of their private health information will be transmitted to a central, county-operated database.

4. Accessing and Amending

Subject to a few exceptions, an individual has a right of access to inspect and obtain a copy of most of her own PHI for as long as the information is maintained by the entity. The regulation carefully outlines each of the exceptions to this access requirement and prescribes procedures for denying a request for access.

Once an individual has accessed her information, she may conclude that the information is inaccurate or incomplete. If so, she may request that the entity make amendments to that information. If the entity accepts the request, in addition to making the amendment it must notify other entities to whom it has disclosed the information. If the entity denies the request, the regulation outlines specific procedures that must be followed, such as permitting the individual to file a statement of disagreement with the contested information.

CAP grantee networks will need to develop a system for managing requests for inspection and amendment. To the extent that CAP funds are being used to develop a common information system, the system design should incorporate a mechanism to track requests for inspection and amendment. Properly designed, such a system could greatly relieve the administrative burden on providers.

5. Receiving an Accounting of Disclosures

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity anytime in the past six years. Certain types of disclosures are not required to be included in the accounting, including disclosures for treatment, payment and health care operations. The accounting must specify the date of the disclosure, who received the information and why it was disclosed. For example, if the state has a disease registry program and the provider has disclosed individually identifiable health information to that registry as required by law, the patient may come back later and ask for an accounting for the disclosure. Consequently,

the provider should be prepared to tell the patient who received the information, what information was provided and what the basis was for the release.

Many new information systems are able to generate an accounting – or "footprint" – for a medical record. Grantee networks that are instituting new systems should explore whether their system is able to produce such a report and, if so, whether it can be configured to capture all of the specific information that is required by the regulation.

F. What New Administrative Measures Are Required?

Covered entities will be required to implement several administrative measures. Each entity will need to develop privacy policies and procedures that reflect the requirements of the privacy regulation (and any other applicable privacy laws) and appoint a privacy official who is responsible for implementing those policies and procedures. The entity will also be required to train employees, volunteers and others who will be using PHI in the course of their work and develop a system for sanctioning employees who violate the entity's policies and procedures. A covered entity will also be required to have a system for receiving complaints from individuals, including the designation of a person or office responsible for receiving such complaints.

Each entity will also be required to have in place appropriate administrative, technical, and physical safeguards, and the entity must reasonably protect PHI from any intentional or unintentional use or disclosure. The "safeguard" requirement in the privacy regulation only imposes general requirements; it is expected that the final security regulation will build on these same general requirements by directing entities to take specific steps to safeguard information. It is possible that in order for an entity to be in compliance with the safeguard requirements of the privacy rule, it will also need to be in compliance with the final security regulation.

G. What Are The Penalties For Noncompliance?

The penalties for *unintentional* violations of the privacy regulations are not nearly as severe as some other federal enforcement regimes, such as the False Claims Act, but they are still significant. Providers are liable for civil monetary penalties of $100 for each incident of violating a standard in the regulation up to a maximum of $25,000 aggregate per year per standard. Because one action can violate multiple requirements, these penalties can become higher than they might initially seem. HIPAA also provides for federal criminal penalties for *intentional* disclosures. Criminal penalties are up to $50,000 and one year in prison for knowingly obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

H. How Does This Regulation Affect State Privacy Laws?

HIPAA carefully defines how this regulation will affect state laws. As a general rule, this federal regulation does not preempt any state privacy law that is more stringent than the regulation. There are several specific types of laws that are exempt from preemption, including child abuse reporting, birth and death reporting, and certain reporting requirements applicable to health plans. HIPAA also permits the Secretary to make determinations that other laws are not preempted, such as certain laws relating to controlled substances, fraud and abuse, and insurance regulation.

III. INFORMATION SHARING FOR CAP GRANTEES

CAP is specifically intended to encourage collaboration among providers for the uninsured. Many grantees have proposed collaborations that rely upon innovative systems for sharing patient information and coordinating care. Through these systems, communities will be able to increase access to health care services for the uninsured and improve quality of care. However, grantees and participants should be aware of how these systems can present risks to patient privacy and also understand what steps they should take to ensure that plans and providers participating in the grant are in compliance with applicable laws, including the HIPAA privacy regulation.

As explained above, providers of direct care to patients will be required to obtain an individual's consent for treatment, payment and health care operations. This consent is only valid for the use and disclosure of PHI by the individual provider receiving the consent – the clinic, hospital or practitioner. It does not permit the use or disclosure by any other entity. For example, if one provider needs PHI from another provider, it cannot rely on a consent to get information from that other provider. Therefore, the key problem for many networks funded by CAP is as follows:

> John Smith is uninsured and has been treated by Provider A and Provider B. He signed consent forms at both offices, so both providers may use and disclose the information that they personally received for John's care. Assuming Provider A and Provider B want to input John's health information into an integrated medical record system, the consent permits each provider to enter the information that they each collect into the system, but they will each only be permitted to use the information that they personally received in caring for John. The consent John signed for Provider A does not permit Provider B to *use* the information that Provider A collected.

Given this regulatory framework, how will CAP grantee networks be able to share information in order to achieve their goal of coordinating care for the uninsured?

Without an individual's authorization, the two providers will only be permitted to share PHI received for treatment or payment in order to coordinate John's care:

- If one provider is a business associate of the other provider;

- If the providers are "affiliated"; or

- If the providers are involved in an organized health care arrangement and they are using joint consents and joint notices.

If the providers do not fall into one of these three categories, they must obtain an authorization.

1. Are the Participants Business Associates?

As explained above, an entity is a business associate if it performs a function on behalf of the covered entity or if it uses PHI to perform specific services for the covered entity, such as legal or financial services. Therefore, the two providers will not be business associates if they are merely sharing information. For example, a hospital and a member of its medical staff are not necessarily business associates of each other. One entity must be performing a function on behalf of the other entity. For instance, if a hospital assumes responsibility for scheduling visits at a clinic, it becomes the business associate of that clinic. The patient consent for the *clinic* must be broad enough to cover the use of PHI by the hospital in its role as business associate.

2. Are the Participants "Affiliated"?

The regulation recognizes that certain groups of covered entities may be treated as a single entity under limited circumstances. If entities are legally separate but are subject to common ownership or control, they may designate themselves as a single entity for purposes of the regulation. Common ownership exists if an entity has an ownership or equity interest of 5% or more in another entity. Common control exists if an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity.

Because providers participating in a CAP grant are most often a broad mix of public and private clinics and hospitals, local health departments, and physician practices, it is unlikely that all participants could be considered affiliated entities because they would not be subject to either common ownership or control.

3. Are the Participants Part of an "Organized Health Care Arrangement"?

In order to allow information to flow more freely in certain situations, the regulation creates the concept of an "organized health care arrangement." An organized health care arrangement would be:

- A clinically integrated care setting in which individuals typically receive care from more than one provider; or

- An organized system of health care in which more than one covered entity participates and in which the entities hold themselves out to the public as a joint arrangement and

participate in at least one of the following activities: utilization review, quality assessment and improvement activities, or payment activities in which the entities share financial risk.

An example of the first type of arrangement might be a hospital that provides physicians with staff privileges or has a separate emergency department. In both of these situations, the hospital could be covered under the regulation separately from the providers (the physicians or emergency department), but because they are clinically integrated, the regulation will recognize them as an organized health care arrangement. An example of the second type of arrangement would be an independent practice association (IPA) formed by a group of physicians. These physicians may hold themselves out as a single entity, but they may not practice in the same setting or share financial risk. As long as the physicians participate in one of the activities identified in the regulation, they may be classified as an organized health care arrangement. The key to these arrangements, according to DHHS, is that individuals who obtain services from them have an expectation that the providers are integrated and that they jointly manage their operations.

There are several benefits to being part of an organized health care arrangement. The regulation affords unique flexibility in a few specific areas: They are allowed to use a joint consent form and a joint notice of privacy practices; they do not need to comply with the requirements for business associate contracts for other entities in the arrangement; and they are all permitted to share information for treatment, payment and health care operations with other entities in the arrangement. It is this last issue that is particularly important; if different entities are able to share information freely for treatment, payment and health care operations, it will be much easier to coordinate care and increase efficiencies in the delivery of health services. For example, providers may want to combine patient information in order to develop treatment protocols. If they are not in an organized health care arrangement, they will be required to obtain an individual's authorization for this information sharing.

The question for CAP grantee networks is whether the provider participants could be considered an organized health care arrangement and, if so, whether they should take advantage of the flexibility afforded to these arrangements. It is certainly possible that the participants, or at least a few of the participants, could fall within this category. For example, the grantee may be developing a managed care program for the uninsured population in the community. If the managed care program is clearly identified to the public as a joint venture and all of the providers participate in joint quality improvement activities, the program could be considered an organized health care arrangement.

4. What Rules Apply to an Organized Health Care Arrangement?

If the CAP grantee network does qualify as an organized health care arrangement, the participant must consider whether it should take advantage of the flexibility available under that category. In order to do so, the entities would need to have a joint consent form and a joint notice. Joint consents and notices could potentially serve to simplify a lot of the administrative burden for each of the entities, but they could also present some problems. Each of the entities will have many unique uses and disclosures that would need to be identified in the notice. For

example, a health center may be required to disclose patient information to HRSA in connection with an evaluation of its performance under a Section 330 grant, and a local health department may use patient information for public health surveillance activities or investigations. Any joint notice for the two entities would need to include all of these unique uses and disclosures in order to be valid.

The benefits of such an arrangement would be the ease of sharing information among participants for treatment, payment and health care operations. Without qualifying as an organized health care arrangement, participants in CAP grant will most likely need to rely on individual authorizations in order to share information for the purpose of coordinating and integrating care.

5. What Rules Apply to Obtaining an Authorization?

If the providers do not fall into any of the three categories described above – affiliates, business associates, or organized health care arrangement – they will be required to obtain an individual's authorization in order to share PHI for use in providing treatment, obtaining payment or conducting health care operations. As explained above, an authorization is a completely separate document from the consent and it has several different requirements and restrictions.

The regulation specifies particular elements that must be included in order for the authorization to be valid. All authorizations must include certain core elements, including a specific and meaningful description of the information to be used or disclosed, a signature, and an expiration date or event that relates to the individual or the purpose of the use or disclosure. If, as in the John Smith example cited above, Provider A is requesting an authorization that will allow Provider B to disclose information to A for treatment, payment or health care operations, the authorization is required to include the core elements just described as well as several additional elements. The additional elements include:

- A description of each purpose of the requested disclosure;
- A statement that the entity will not condition treatment, payment, enrollment or eligibility on the authorization (except in limited circumstances); and
- A statement that the individual may refuse to sign the authorization.

These last two elements are extremely significant and highlight one of the key differences between authorizations and consents. An entity may condition treatment or enrollment in a health plan on obtaining a consent. By contrast, an entity is not permitted to condition treatment, payment, enrollment in a plan, or eligibility for benefits on an authorization except in limited circumstances. Therefore, an individual in need of health care is highly likely to sign a consent but he may be much more reluctant to sign an authorization. This could present problems for CAP grantee networks that rely upon data sharing arrangements.

The regulation allows for a single authorization to be used to enable disclosures by a "class of persons" as long as the class is identified with sufficient specificity. Therefore, when John Smith visits Provider A, who contributes information to an integrated medical records system, Provider A could present him with a single authorization that identifies all of the other participants in the system (Providers B-Z) and authorizes all of those other entities to disclose information to Provider A for treatment, payment and health care operations. Alternatively, Provider A could ask John to sign separate authorization forms for each source of information. While this would be more cumbersome, the regulation does allow these authorizations to be combined in a single document as long as the entity has not conditioned the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the provision of any one of the authorizations.

Subject to limited exceptions, an individual may revoke authorizations at any time. Authorizations are also required to have expiration dates or events. CAP networks that rely upon authorizations in order to share information will need to have a system in place for tracking these authorizations in order to modify access to PHI if they have been revoked or if they have expired. For example, if a grantee network has an integrated electronic medical record system, when Provider A obtains an authorization, the system should require Provider A to enter the expiration date into the system and automatically deny access on that date unless a new authorization has been entered. It may be more challenging to develop a means of monitoring revocations.

It is important to note that at the same time Provider A presents John Smith with an authorization, he will also be presenting him with a consent form which will permit Provider A to use and disclose PHI for treatment, payment and health care operations. While consents are not required to have an expiration date or event, they are subject to revocation. Therefore, it will be necessary to set up a system for monitoring those revocations as well.

IV. CONCLUSION

As a reminder, at the time of this briefing, it appears that there may be further changes to the HIPAA privacy regulations. By reopening the regulations to comments, the Department of Health and Human Services has indicated that it will be willing to listen to the provider community's concerns regarding the cost and administrative complexity associated with the regulations. However, it is unlikely that the Administration will reject the bulk of the provisions in the regulations. A more likely scenario is that there will be some tinkering at the edges.

Consequently, CAP grantees will still need to plan on HIPAA compliance. At a minimum, when purchasing information systems and negotiating business relationships with other providers or vendors, they need to lay a foundation for HIPAA privacy compliance.

::ODMA\PCDOCS\WSH\210807\1