HIPAA Privacy FAQ's

1. What is the HIPAA privacy regulation?

Until Congress passed HIPAA in 1996, personal health information (PHI) was protected by a patchwork of federal and state laws. Patients' health information could be distributed without their consent for reasons having nothing to do with their medical treatment or health care reimbursement. The HIPAA regulation provides the first comprehensive federal protection for the privacy of individually identifiable health information (IIHI). The regulation increases consumer control over the use and disclosure of their medical information. It also establishes appropriate safeguards that must be followed to protect the privacy of patients' health information.

2. What does the HIPAA Privacy Rule do?

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- It strikes a balance when public responsibility supports disclosure of some forms of data.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how PHI may be used.

- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonable needed for the purpose of disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

3. Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

4. Who must comply with these new HIPAA privacy standards?

- Health plans
- Health care clearinghouses
- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

5. What were the major modifications to the HIPAA Privacy Rule that the Department of Health and Human Services (HHS) adopted in August 2002?

Based on the information received through public comments, testimony at public hearings, meetings at the request of industry and other stakeholders, as well as other communications, HHS identified a number of areas in which the Privacy Rule, as issued in December 2000, would have had potential unintended effects on health care quality or access. As a result, HHS proposed modifications that would maintain strong protections for the privacy of individually identifiable health information, address the unintended negative effects of the Privacy Rule on health care quality or access to the health care, and relieve unintended administrative burdens created by the Privacy Rule.

Final modifications to the Rule were adopted on August 14, 2002. Among other things, the modifications addressed the following aspects of the Privacy Rule:

- Uses and disclosures for treatment, payment and health care operations, including eliminating the requirement for the individual's consent for these activities;
- The notice of privacy practices that covered entities must provide to patients;
- Uses and disclosures for marketing purposes;
- Minimum necessary uses and disclosures;
- Parents as the personal representative of un-emancipated minors;
- Uses and disclosures for research purposes; and
- Transition provisions, including business associate contracts.

In addition to these key areas, the modifications included changes to certain other provisions where necessary to clarify the Privacy Rule, and a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

For more information about the final modifications to the Privacy Rule, see the Fact Sheet entitled, *Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule.* This Fact sheet can be found at http://www.hhs.gov/news/press/2002pres/20020809.html

6. Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?

The consent requirement created the unintended effect of preventing health care providers from providing timely, quality health care to individuals in a variety of circumstances. The most troubling and pervasive problem was that health care providers would not have been able to use or disclose PHI for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care.

To eliminate such barriers to health care, mandatory consent was replaced with the voluntary consent provision that permits health care providers to obtain consent for treatment, payment and health care operations, at their option, and enables them to obtain consent in a manner that does not disrupt needed treatment. Although consent is no longer mandatory, the Rule still affords individuals the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded. These modifications will ensure that the Rule protects patient privacy as intended without harming consumers' access to care or the quality of that care. Further, the individual's right to request restrictions on the use or disclosure of his or her PHI is retained in the Rule as modified.

7. Will the Department of Health and Human Services (HHS) make future changes to the HIPAA Privacy Rule and, if so, how will these changes be managed?

Under HIPAA, HHS has the authority to modify the privacy standards as the Secretary may deem appropriate. However, a standard can be modified only once in a 12-month period.

As a general rule, future modifications to the Privacy Rule must be made in accordance with the Administrative Procedure Act (APA). HHS will comply with the APA by publishing proposed rule changes, if any, in the *Federal Register* through a Notice of Proposed Rulemaking and will invite comment from the public. After reviewing and addressing those comments, HHS will issue a modified final rule.

8. What if I don't comply with the regulation?

The government can impose civil penalties for noncompliance ranging from $100 to $250,000 and, in extreme cases, criminal penalties and imprisonment.

9. Can't I just follow state laws regarding physician-patient confidentiality?

No. The HIPAA privacy rule is much more formal than the patient confidentiality laws physicians traditionally adhered to. State law should only be followed when it is more stringent than federal law.

10. What information is protected?

HIPAA defines PHI as individually identifiable health information held or disclosed by a covered entity. PHI is widely inclusive. It can include a patient's name, Social Security number or medical record number; specific dates such as birth, admission, discharge or death; or any other information that may be used to identify a patient. This may include information about past, present or future physical or mental condition, the provision of health care to an individual, or the past, present or future payment for the provision of health care. Simply removing the patient's name is not enough to protect the information, and "de-identification" is an onerous task that most physician practices will not undertake.

11. Do I only have to protect the PHI that is transmitted electronically?

No. If you are a covered entity (CE), all uses and disclosures of PHI are regulated. You must institute safeguards to protect PHI whether you disclose it verbally, in writing or electronically. The good news is that under the final rule, you do not need the patient's consent for most routine uses or disclosures of PHI related to treatment, payment and health care operations (TPO). Health care operations include but are not limited to fundraising activities; quality assessment and improvement activities; insurance activities; business planning, development and management activities, licensing and audits; evaluating health care professionals and plans; and training health care professionals.

12. What are the basic rules on disclosure of PHI?

The rules regarding the use of PHI pertain to disclosures as well. Essentially, your practice may use and disclose PHI for your own TPO activities. The regulation also requires that you put in place policies regarding use and disclosure.

13. What kinds of safeguards are required?

You must establish appropriate administrative, technical and physical safeguards to protect PHI in your practice from intentional or unintentional disclosure. For example, the regulation requires you to limit access to PHI but provides you with enough flexibility to determine for yourself who in your office needs access to PHI and how much information they need to do their jobs.

14. What are a patient's rights regarding PHI?

Patients have six fundamental rights:

1. The right to receive a notice about your privacy policies.
2. The right to access the medical information you maintain about him or her.
3. The right to limit the uses and disclosures of medical information.
4. The right to request amendments to the medical record.
5. The right to revoke or limit authorization.
6. The right to an accounting of disclosures of PHI.

15. What should I do to protect the PHI in my office?

Although the privacy regulation gives you some flexibility for determining what is reasonable for protecting PHI in your office, you will be required to do the following:

- Adopt clear privacy policies and procedures for your practice.
- Designate someone to be responsible for seeing that the privacy policies and procedures are followed.
- Train employees so that they understand the privacy policies and procedures.
- Secure patient records containing PHI so that they are not accessible to those who don't need them.
- Provide information to patients about their privacy rights and how their information can be used.

16. What are some practical first steps?

- Develop privacy policies and procedures.
- Identify business associates.
- Develop a privacy notice**.**
- Decide how you will give notice.
- Determine authorization needs.
- Decide how you will handle requests for PHI.
- Develop a system for managing restrictions on PHI.
- Develop a procedure for logging disclosures.

17. If I believe that my privacy rights have been violated, when can I submit a complaint?

By law, covered entities have until April 14, 2003 to comply with the Privacy Rule. Small health plans have until April 14, 2004 to comply. Activities occurring before Aril 14, 2003, are not subject to the Office for Civil Rights (OCR) enforcement actions. After that date, a person who believes a covered entity is not complying with a requirement of the Privacy Rule may file with OCR a written complaint, either on paper or electronically. This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred. The Secretary may waive this 180-day time limit if good cause is shown.

In addition, after the compliance dates above, individuals have a right to file a complaint directly with the covered entity. Individuals should refer to the covered entity's notice of

privacy practices for more information about how to file a complaint with the covered entity.

18. Can a physician's office fax patient medical information to another physician's office?

The Privacy Rule permits physicians to disclose PHI to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI that is disclosed using a fax machine.

19. Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures. Reasonable precautions could include using lowered voices or talking apart from others when sharing PHI. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

20. May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?

Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addtion, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine.

A covered entity may also leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered

entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable.

21. A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the HIPAA Privacy Rule allow the hospital to continue this practice?

The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure. In this case, disclosure of patient names, by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment, or health care operations purposes. The disclosure of such information to other persons that will likely also occur due to the posting is an incidental disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate.

22. May mental health practitioners or other specialists provide therapy to patients in a group setting where other patients and family members are present?

Yes. Disclosures of PHI in a group therapy setting are treatment disclosures and, thus, may be made without an individual's authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose PHI to a family member or other person involved in the individual's care. Where the individual is present during the disclosure, the covered entity may disclose PHI if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual's agreement to participate in group therapy or family discussions is a good basis for inferring the individual's agreement.

23. Can physician offices use patient sign-in sheets or call out the names of patients in their waiting rooms?

Yes, covered entities such as physician offices may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The Privacy Rule explicitly permits certain "incidental disclosures" that occur as a by-product of an otherwise permitted disclosure. However, these "incidental" disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards, and implemented the minimum necessary standard, where appropriate.

24. Are hospitals able to inform the clergy about parishioners in the hospital?

Yes, the Privacy Rule allows this communications to occur, as long as the patient has been informed of this use and disclosure, and does not object. The Privacy Rule provides that a hospital or other covered health care provider may maintain in a directory the following information about that individual: the individual's name; location in the facility; health condition expresses in general terms; and religious affiliation. The facility may disclose this directory information to members of the clergy.

25. 25. Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?

No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

26. Are covered entities required to document incidental disclosures permitted by the HIPAA Privacy Rule, in an accounting of disclosures provided to an individual?

No. The Privacy Rule includes a specific exception from the accounting standard for incidental disclosures permitted by the Rule.

27. Is a covered entity required to prevent any incidental use or disclosure of PHI?

No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures.

28. How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and

guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.

The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to PHI. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to PHI without sacrificing the quality of health care.

29. Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?
No. Disclosures for treatment purposes between health care providers are explicitly exempted from the minimum necessary requirements.

30. Does the Privacy Rule's minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training?

No. The definition of "health care operations" in the Privacy Rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records.

31. Must the Privacy Rule's minimum necessary standard be applied to uses or disclosures that are authorized by an individual?

No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements. However, the authorization must meet the requirements of 45 CFR 164.508.

32. Does the Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time an entire medical record is disclosed?

No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a covered entity may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and

requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes.

The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who is the subject of the PHI.

33. A provider might have a patient's medical records that contain older portions of a medical record that were created by another or previous provider. Will the Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

34. Is a covered entity required to apply the HIPAA Privacy Rule's minimum necessary standard to a disclosure of PHI it makes to another covered entity?

Covered entities are required to apply the minimum necessary standard to their own requests for PHI. One covered entity may reasonably rely on another covered entity's request as the minimum necessary, and then does not need to engage in a separate minimum necessary determination.

However, if a covered entity does not agree that the amount of information requested by another covered entity is reasonably necessary for the purpose, it is up to both covered entities to negotiate a resolution of the dispute as to the amount of information needed. Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with another covered entity making a request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.

35. Do hospitals or other covered entities need to monitor their business associates?

No, the Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of PHI; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract.

36. Are State, county, or local health departments required to comply with the Privacy Rule?

Yes, if a State, county or local health department performs functions that make it a covered entity, or otherwise meets the definition of a covered entity. Some health care departments operate health care clinics and thus are health care providers. If these health care providers transmit health information electronically in connection with a transaction covered in the HIPAA Transaction Rule, they are covered entities.

37. The Social Security Administration (SSA) collects medical records for the Social Security Income (SSI) disability program. Is SSA a covered entity?

The SSA is not a covered entity. The collection of individually identifiable health information is not a factor in determining whether an entity is a covered entity. Covered entities are defined in HIPAA; they are (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transactions Rule.

38. Does the HIPAA Privacy Rule change the way in which an individual can grant another person health care power of attorney?

No. Nothing in the Privacy Rule changes the way in which an individual grants another person power of attorney for health care decisions. State law (or other law) regarding health care powers of attorney continue to apply. The intent of the provisions regarding personal representatives was to complement, not interfere with or change, current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions, which give others the ability to exercise the rights of, or make treatment decisions related to, an individual. The Privacy Rule provisions regarding personal representatives generally grant persons, who have authority to make health care decisions for an individual under the law, the ability to exercise the rights of that individual with respect to health information.

39. Can the personal representative of an adult or emancipated minor obtain access to the individual's medical record?

The HIPAA Privacy Rule treats an adult or emancipated minor's personal representative as the individual for purposes of the Rule regarding the health care matters that relate to the representation, including the right of access under 45 CFR 164.524. The scope of access will depend on the authority granted to the personal representative by other law. If the personal representative is authorized to make health care decisions, generally, then the personal representative may have access to the individual's PHI regarding health care in general. On the other hand, if the authority is limited, the personal representative may have access only to PHI that may be relevant to making decisions within the personal representative's authority.

There is an exception to the general rule that a covered entity must treat an adult or emancipated minor's personal representative as the individual. Specifically, the Privacy Rule does not require a covered entity to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or

may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. This exception applies to adults and both emancipated and un-emancipated minors who may be subject to abuse or neglect by their personal representatives.

40. How can family members of a deceased individual obtain the deceased individual's PHI that is relevant to their own health care?

The HIPAA Privacy Rule recognizes that a deceased individual's PHI may be relevant to a family member's health care. The Rule provides two ways for a surviving family member to obtain the PHI of a deceased relative. First, disclosures of PHI for treatment purposes – even the treatment of another individual – do not require authorization; thus, a covered entity may disclose a decedent's PHI, without authorization, to the health care provider who is treating the surviving relative. Second, a covered entity must treat a deceased individual or his estate, as a personal representative with respect to PHI relevant to such representation. Therefore, if it is within the scope of such personal representative's authority under other law, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure.

41. Does the HIPAA Privacy Rule address when a person may not be the appropriate person to control an individual's PHI?

Generally, no. The Rule defers to State and other laws that address the fitness of a person to act on an individual's behalf. However, a covered entity does not have to treat a personal representative as the individual when it reasonably believes, in the exercise of professional judgment, the individual is subject to domestic violence, abuse or neglect by the personal representative, or doing so would otherwise endanger the individual.

42. May adults with mental retardation control their PHI if they are able to authorize uses and disclosures of their PHI?

Individuals may control their PHI under the HIPAA Privacy Rule to the extent State or other law permits them to act on their own behalf. Further, even if an individual is deemed incompetent under State or other law to act on his or her own behalf, covered entities may decline a request by a personal representative for PHI if the individual objects to the disclosure (or for any other reason), and the disclosure is merely permitted, but not required, under the Rule.

However, covered entities must make disclosures that are required under the Rule. Consequently, with respect to the individual's right of access to PHI and for an accounting of disclosures, covered entities must provide the individual's personal representative access to the individual's PHI or an accounting of disclosures upon the request of the personal representative, unless the covered entity, in the exercise of professional judgment, believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual may be subject to domestic

violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. The Rule allows a specified time period before a covered entity must act on such a request; and during this interim period, an individual and his personal representative will have an opportunity to resolve any dispute they may have concerning the request.

43. Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?

Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law.

There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are: (1) when the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law; (2) when the minor obtains care at the direction of a court or a person appointed by the court; and (3) when, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship. However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent's right of access in these cases, the licensed health care provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonable believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.

44. May a psychologist continue his practice to notify a parent before treating his or her minor child, even though the minor child is able to consent to such health care under State law?

The HIPAA Privacy Rule would defer to State or other applicable law that addresses the disclosure of health information to a parent about a minor child. If the minor child is permitted, under State law, to consent to such health care without the consent of her parent and does consent to such care, the provider may notify the parent when the State law explicitly requires or permits the health care provider to do so. If State law permits the minor child to consent to such health care without parental consent, but is silent on parental notification, the provider would need the child's permission to notify a parent.

45. Has the Secretary exceeded the HIPAA statutory authority by requiring "business associates" to comply with the Privacy Rule, even if that requirement is through a contract?

The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing PHI to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the covered entity comply with its obligations under the Rule.

Business associates, however, are not subject to the requirements of the Privacy rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business contract with the covered entity, unless the business associate is itself a covered entity.

46. What are a covered entity's obligations under the HIPAA Privacy Rule with respect to PHI held by a business associate during the contract transition period?

During the contract transition period, covered entities must observe the following responsibilities with respect to PHI held by their business associates:

- Make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity.
- Fulfill an individual's right to access and amend his or her PHI contained in a designated record set, including information held by a business associate, if appropriate, and receive an accounting of disclosures by a business associate.
- Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of an impermissible use or disclosure of PHI by its business associate.

Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.

However, a covered entity is not required to obtain the satisfactory assurances required by the Privacy Rule from a business associate to which the transition period applies.

Of course, even during the transition period, covered entities still may only disclose PHI to a business associate for a purpose permitted under the Rule and must apply the minimum necessary standard, as appropriate, to such disclosures.

47. I have an existing contract with a business associate that will renew automatically before April 14, 2003. Does this automatic renewal mean I have to modify the contract by April 14, 2003, to make it compliant with the HIPAA Privacy Rule's

business associate contract provisions or can I still take advantage of the transition period?

Evergreen or other contracts that renew automatically without any change in terms or other action by the parties and that exist by October 15, 2002, are eligible for the transition period. The automatic renewal of a contract itself does not terminate qualification for the transition period, or the transition period itself. Renewal or modification for the purposes of the transition provisions requires action by the parties involved.

48. Is a covered entity liable for, or required to monitor, the actions of its business associates?

No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of PHI; but covered entities are not required to monitor or oversee the means by which their business associate abides by the privacy requirements of the contract. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible, the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights.

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule, if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of PHI to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out f compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

49. Is a business associate contract required for a covered entity to disclose PHI to a researcher?

No. Disclosures from a covered entity to a researcher for research purposes do not require a BA contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103. However, the Privacy Rule does not prohibit a CE from entering into a BA contract with a researcher if the CE wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose PHI to a researcher as permitted by the Rule, that is, with an individual's authorization pursuant to 45 CFR 164.508, without an individual's authorization as permitted by 45 CFR

164.512(i) or as a limited data set provided that a data use agreement is in places as permitted by 45 CFR 164.514(e).

50. May a covered entity share PHI directly with another covered entity's business associate?

Yes. If the HIPAA Privacy Rule permits a covered entity to share PHI with another covered entity, the covered entity is permitted to make the disclosure directly to a business associate acting on behalf of that other covered entity.

51. Is a BA contract required with organizations or persons where inadvertent contact with PHI may result – such as in the case of janitorial services?

A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of PHI, and any performances of their duties is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonable prevented.

If a service is hired to do work for a covered entity where disclosure of PHI is not limited in nature, it likely would be a business associate. However, when such work is performed under the direct control of the CE, the Privacy Rule permits the CE to treat the service as part of its workforce, and the CE need not enter into a BA contract with the service.

52. Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their PHI or an accounting of disclosures, or an opportunity to amend PHI?

The Privacy Rule regulates covered entities, not business associates. The Rule requires covered entities to include specific provisions in agreements with business associates to safeguard PHI, and addresses how covered entities may share this information with business associates. Covered entities are responsible for fulfilling Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting. With limited exceptions, a covered entity is required to provide an individual access to his or her PHI in a designated record set. Therefore, the Rule requires covered entities to specify in the BA contract that the BA must make such PHI available if and when needed by the CE to provide an individual with access to the information.

Under 45 CFR 164.526, a covered entity must amend PHI about an individual in a designated record set, including any designated record sets held by a BA.

Under 45 CFR 164.528, the Privacy Rule requires a CE to provide an accounting of certain disclosures, including certain disclosures by its BA, to the individual upon request.

53. Would a BA contract in electronic form, with an electronic signature, satisfy the HIPAA Privacy Rule's BA contract requirements?

Yes, assuming that the electronic contract satisfies the applicable requirements of State contract law. The Privacy Rule generally allows for electronic documents, including BA contracts, to qualify as written documents for purposes of meeting the Rule's requirements. However, currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, covered entities must ensure any electronic signature used will result in a legally binding contract under applicable State or other law.

54. I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data use agreement and business associate contract?

Yes. A data use agreement can be combined with a BA into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule. In the above situation, because the CE is providing the recipient with PHI that includes direct identifiers, a BA agreement would be required in addition to the data use agreement to protect the information.

55. If the only PHI a BA receives is a limited data set, does the HIPAA Privacy Rule require the CE to enter into both a BA agreement and data use agreement with the BA?

No. Where a CE discloses only a limited data set to a BA for the BA to carry out a health care operations function, the CE satisfies the Rule's requirements that it obtain satisfactory assurances from its BA with the data use agreement.

56. How does the HIPAA Privacy Rule change the laws concerning consent for treatment?

The Privacy Rule relates to uses and disclosures of PHI, not to whether a patient consents to the health care itself. As such, the Privacy Rule does not affect informed consent for treatment, which is addressed by State law.

57. What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule?

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of PHI for treatment, payment and health care operations (TPO). Covered entities that do so have complete discretion to design a process that best suits their needs.

By contrast, an "authorization" is required by the Privacy Rule for uses and disclosures of PHI not otherwise allowed by the Rule. Where the Privacy Rule requires patient

authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. An authorization must specify a number of elements, including a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the CE may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

58. Does the HIPAA Privacy Rule permit a covered entity or its collection agency to communicate with parties other than the patient regarding payment of a bill?

Yes. The Privacy Rule permits a covered entity, or a business associate acting on behalf of a CE, to disclose PHI as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. Therefore, a CE, or its BA, may contact persons other than the individual as necessary to obtain payment for health care services. However, the Privacy Rule requires a CE, or its BA, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to-restrictions on the use or disclosure of PHI.

59. Can a pharmacist use PHI to fill a prescription that was telephoned in by a patient's physician without the patient's written consent if the patient is a new patient to the pharmacy?

Yes. The pharmacist is using the PHI for treatment purposes, and the HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing PHI about him or her for treatment, payment or health care operations (TPO).

60. Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use PHI to set up appointments or schedule surgery or other procedures without the patient's consent?

Yes. The HIPAA Privacy Rule does no require covered entities to obtain an individual's consent prior to using or disclosing PHI about him or her for treatment, payment, or health care operations.

61. Are health care providers restricted from consulting with other providers about a patient's condition without the patient's written authorization?

No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule's definition of "treatment" and, therefore is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose PHI about an individual to a health care provider for that provider's treatment of the individual.

62. How does the HIPAA Privacy Rule apply to professional liability insurance? Specifically, how can professional liability insurers continue to arrange for and maintain medical liability insurance for health care providers covered by the Rule?

The Privacy Rule permits a covered health care provider to disclose information for "health care operations" purposes, subject to certain requirements. Disclosures by a covered health care provider to a professional liability insurer or a similar entity for the purpose of obtaining or maintaining medical liability coverage or for the purpose of obtaining benefits from such insurance, including the reporting of adverse events, fall within "business management and general administrative activities" under the definition of "health care operations." Therefore, a covered health care provider may disclose individually identifiable health information to a professional liability insurer to the same extent as the provider is able to disclose such information for other health care operations purposes.

63. Can contractors (business associates) use PHI to market to individuals for their own business purposes?

No. While covered entities may share PHI with their contractors who meet the definition of "business associates" under the HIPAA Privacy Rule, that definition is limited to contractors that obtain PHI to perform or assist in the performance of certain health care operations on behalf of covered entities. Thus, business associates, with limited exceptions, cannot use PHI for their own purposes. Although, under the HIPAA statute, the Privacy Rule cannot govern contractors directly, the Rule does set clear parameters for how covered entities may contract with business associates.

Further, the Privacy Rule expressly prohibits health plans and covered health care providers from selling PHI to third parties for the third party's own marketing activities, without authorization.

64. When is an authorization required from the patient before a provider or health plan engages in marketing to that individual?

The HIPAA Privacy Rule expressly requires an authorization for uses or disclosures of PHI for ALL marketing communications, except in two circumstances: (1) when the communication occurs in a face-to-face encounter between the covered entity and the individual; or (2) the communication involves a promotional gift of nominal value.

If the marketing communication involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

65. How can I distinguish between activities for treatment or health care operations versus marketing activities?

The overlap among common usages of the terms "treatment," "health care operations," and "marketing" is unavoidable. The Privacy Rule defines these terms specifically, so they can be distinguished. For example, the Privacy Rule excludes treatment communications and certain health care operations activities from the definition of "marketing." If a communication falls under one of the definition's exceptions, the marketing rules do not apply. In these cases, covered entities may engage in the activity without first obtaining an authorization.

However, if a health care operation communication does not fall within one of these specific exceptions to the marketing definition, and the communication falls under the definition of "marketing," the Privacy Rule's provisions restricting the use or disclosure of PHI for marketing purposes will apply. For these marketing communications, the individual's authorization is required before a covered entity may use or disclose PHI.

66. Do disease management, health promotion, preventive care, and wellness programs fall under the HIPAA Privacy Rule's definition of "marketing"?

Generally, no. To the extent the disease management or wellness program is operated by the covered entity directly or by a business associate, communications about such programs are not marketing because they are about the covered entity's own health related services.

Moreover, a communication that merely promotes health in general manner and does not promote a specific product or service from a particular provider does not meet the definition of "marketing." Such communications may include population-based activities in the areas of health education or disease prevention. Examples of general health promotional material include mailings reminding women to get an annual mammogram; mailings providing information about how to lower cholesterol, new developments in health care, support groups, organ donation, cancer prevention, and health fairs.

67. Is it "marketing" for a covered entity to describe products or services that are provided by the covered entity to its patients, or to describe products or services that are included in the health plan's plan of benefits to members of the health plan?

No. The HIPAA Privacy Rule excludes from the definition of "marketing" communications made to describe a covered entity's health-related product or service that is provided by, or included in a plan of benefits of, the covered entity making the communication.

68. Is it marketing for an insurance plan or health plan to send enrollees notices about changes, replacements, or improvements to existing plans?

No. The HIPAA Privacy Rule excludes from the definition of "marketing," communications about replacements of, or enhancements to, a health plan. Therefore, notices about changes in deductibles, co-pays and types of coverage are not marketing.

Likewise, a notice to a family warning that a student reaching the age of majority on a parental policy will lose coverage, then offering continuation coverage, would not be considered marketing. Nor are special health care policies such as guaranteed issue products and conversion policies considered marketing. Similarly, notices from a health plan about its long term benefits would not be considered marketing.

69. Can a doctor or pharmacy be paid to make a prescription refill reminder without prior authorization under the HIPAA Privacy Rule?

Yes. It is not marketing for a doctor to make a prescription refill reminder even if a third party pays for the communication. The prescription refill reminder is considered treatment. The communication is therefore excluded from the definition of marketing and does not require a prior authorization. Similarly, it is not marketing when a doctor or pharmacy is paid by a pharmaceutical company to recommend an alternative medication to patients. Communications about alternative treatments are excluded from the definition of marketing and do not require a prior authorization. The simple receipt of remuneration does not transform a treatment communication into a commercial promotion of a product or service.

Furthermore, covered entities may use a legitimate business associate to assist them in making such permissible communications. However, a covered entity would require an authorization if it sold PHI to a third party for the third party's marketing purposes.

70. Are appointment reminders allowed under the Privacy Rule without authorizations?

Yes, appointment reminders are considered part of treatment of an individual and, therefore, can be made without an authorization.

71. What are examples of "alternative treatments" that are excepted from the HIPAA Privacy Rule's definition of "marketing"?

Alternative treatments are treatments that are within the range of treatment options available to an individual. For example, it would be an alternative treatment communication if a doctor, in response to an inquiry from a patient with a skin rash about the range of treatment options, mails the patient a letter recommending that the patient purchase various ointments and medications described in brochures enclosed with the letter. Alternative treatment could also include alternative medicine. Thus, alternative treatments would include communications by a nurse midwife who recommends or sells vitamins and herbal preparations, dietary and exercise programs, massage services, music or other alternative types of therapy to her pregnant patients.

72. What effect do the "marketing" provisions of the HIPAA Privacy Rule have on Federal or State fraud and abuse statutes?

The Privacy Rule makes it clear that nothing in the marketing provisions of the Privacy Rule are to be construed as amending, modifying, or changing any rule or requirement related to any other Federal or State statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations.

73. May covered entities use information regarding specific clinical conditions of individuals in order to communicate about products or services for such conditions without a prior authorization?

Yes, if the communication is for the individual's treatment or for case management, care coordination, or the recommendation of alternative therapies. The HIPAA Privacy Rule permits the use of clinical information to the extent it is reasonable necessary for these communications. Similarly, population-based activities in the areas of health education or disease prevention are not considered marketing when they promote health in a general manner. Again clinical information may be used for such communications, such as in targeting a public education campaign.

74. Must a health care provider or other covered entity obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease?

No. All States have laws that require providers to report cases of specific diseases to public health officials. The Privacy Rule permits disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affected by a disease. In some cases they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public.

75. Must a health care provider or other covered entity obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease?

No. All States have laws that require providers to report cases of specific diseases to public health officials. The Privacy Rule permits disclosures that are required by law. Disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affect by a disease. In some cases, they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

76. May covered entities disclose facially identifiable PHI, such as name, address, and social security number, for public health purposes?

Yes. The HIPAA Privacy Rule permits covered entities to disclose the amount and type of PHI that is needed for public health purposes. In some cases, the disclosure will be required by other law, in which case, covered entities may make the required disclosure pursuant to 45 CFR 164.512 (a) of the Rule. For disclosures that are not required by law, covered entities may disclose, without authorization, the information that is reasonable limited to that which is minimally necessary to accomplish the intended purpose of the disclosure. For routine or recurring public health disclosures, a covered entity may develop protocols as part of its minimum necessary policies and procedures to address the type and amount of information that may be disclosed for such purposes. Covered entities may also rely on the requesting public health authority's determination of the minimally necessary information.

77. To whom may covered entities make public health disclosures regarding a produce regulated by the Food and Drug Administration (FDA) when more than one person is identified on the product label?

Covered entities may identify persons responsible for an FDA-regulated product by using the product label, the literature that accompanies the product, or other sources of labeling, such as the Physician's Desk Reference. If multiple persons are named, covered entities may choose any of the persons named by these sources.

78. Does the HIPAA Privacy Rule's public health provision permit covered health care providers to disclose PHI concerning the findings of pre-employment physicals, drug tests, or fitness-for-duty examinations to an individual's employer?

The public health provision permits covered health care providers to disclose an individual's PHI to the individual's employer without authorization in very limited circumstances. First, the covered health care provider must provide the health care service to the individual at the request of the individual's employer or as a member of the employer's workforce. Second, the health care service provided must relate to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury. Third, the employer must have a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the PHI the employer needs to meet such legal obligation may be disclosed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written

notice that the information is to be disclosed to his or her employer (or by posting the notice at the worksite if the service is provided there).

When a health care service does not meet the above requirements, covered entities may not disclose an individual's PHI to the individual's employer without an authorization, unless the disclosure is otherwise permitted without authorization by other provisions of the Rule. However, nothing in the Rule prohibits an employer from conditioning employment on an individual providing an authorization for the disclosure of such information.

79. Are some of the criteria so subjective that inconsistent determinations may be made by Institutional Review Boards (IRB) and Privacy Boards reviewing similar or identical research projects?

Under the HIPAA Privacy Rule, IRBs and Privacy Boards need to use the judgment as to whether the waiver criteria have been satisfied. Several of the waiver criteria are closely modeled on the Common Rule's criteria for the waiver of informed consent and for the approval of a research study. Thus, it is anticipated that IRBs already have experience in making the necessarily subjective assessments of risks. While IRBs or Privacy Boards may reach different determinations, the assessment of the waiver criteria through this deliberative process is a crucial element in the current system of safeguarding research participants' privacy. The entire system of local IRBs is, in fact, predicated on a deliberative process that permits local IRB autonomy. The Privacy Rule builds upon this principle; it does not change it. Nonetheless, the Department will consider issuing guidance as necessary and appropriate to address concerns that may arise during implementation of these provisions.