

# HIPAA

## Frequently Asked Questions

### 1. What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA's confidentiality provisions, which are collectively known as the Privacy Rule, limit certain participant health care information from improper uses and disclosures.

### 2. What participant information is protected by HIPAA's Privacy Rule?

The Privacy Rule applies to the use and disclosure of Protected Health Information (PHI) by health care providers, health care payors, group health plans, and health care clearinghouses.

### 3. What is protected health information (PHI)?

PHI is any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, or health care clearinghouse, **and** relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual **and** identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

### 4. What is de-identified PHI?

De-identified health information is PHI that has been stripped of its individually identifiable characteristics. Properly de-identified PHI is NOT subject to the Privacy Rule. If de-identified information is subsequently re-identified, it reacquires the Privacy Rule's protections.

### 5. How can PHI be de-identified?

To properly de-identify PHI, it is necessary to remove all identifying characteristics, including -- but not limited to -- participant names, addresses (excluding state and the first three zip code digits), dates (excluding year), Social Security numbers, medical record numbers, telephone and fax numbers, e-mail and other internet addresses, health insurance numbers, identifiable photographs, and other identifying information. Information relating to gender, race, ethnicity, and marital status is not considered individually identifiable and, therefore, may not be removed.

If all identifying characteristics have not been or cannot be removed, PHI may still be treated as de-identified if a qualified statistician examines the PHI and determines the risk of re-identification to be minimal.

## **6. Who must comply with the Privacy Rule?**

The Privacy Rule's legal requirements apply to Covered Entities, such as group health plans.

Covered Entities include all Health Plans, as well as certain Health Care Providers and Health Care Clearinghouses.

A Health Plan, such as a plan sponsor or a health insurance company, provides and/or pays the cost of medical care.

A Health Care Provider is an individual or organization that provides, bills, or is paid for health care services. The Privacy Rule applies only to health care providers who electronically store or transmit PHI in connection with specified health care transactions.

Health Care Clearinghouses, like billing companies, are organizations that process or facilitate the processing of health care transactions.

Some functions, which are not considered covered entities, maintain a HIPAA connection. Such functions include disability, disability pension, and worker's compensation. HIPAA's Privacy Rule affects how covered entities, such as a health care provider, may share or exchange PHI with the disability plan, pension plan or worker's compensation carrier.

## **7. What are Business Associates?**

A Business Associate is an external third party, such as a person or organization, that a covered entity discloses PHI to in order that the third party can carry out or assist in the performance of a function or an activity involving the use or disclosure of individually identifiable health information. This would include but not be limited to: claims processing or administration; legal; accounting; utilization review; quality assurance; billing; benefit management or practice management.

## **8. May group health plans disclose PHI to Business Associates?**

Yes. After a group health plan obtains satisfactory assurances from the Business Associate that it will comply with the Privacy Rule, the group health plan may share PHI with the Business Associate. Obtaining satisfactory assurance means that group health plans must have contracts with their Business Associates that establish the permitted uses and disclosures of PHI.

## **9. Are group health plans liable for Privacy Rule violations committed by their Business Associates?**

Group health plans may be legally responsible for Privacy Rule violations committed by their Business Associates if the group health plan knows about the improper conduct and fails to take reasonable steps to correct it. While a group health plan does not have to actively monitor the conduct of Business Associates, it must conduct an investigation if it learns of possible wrongdoing. If the group health plan cannot, through reasonable efforts, correct a Business Associate's Privacy Rule violation, it must terminate the Business Associate contract. If this is not possible or would cause significant damage to the group health plan's operations, it must report the violation to the U.S. Department of Health and Human Services (HHS).

## **10. What does the Privacy Rule prohibit?**

The Privacy Rule prohibits a group health plan from using or disclosing a participant's PHI for any purpose unless (1) the use or disclosure is permitted or required by the Privacy Rule. Permitted use of PHI includes work required to administer the Health Plan (i.e. participant enrollment, inquiries and communications, and insurance carrier contract administration); or (2) the participant signs a written authorization for the use or disclosure.

## **11. What is the Minimum Necessary standard?**

The Minimum Necessary standard is a rule that requires covered entities to make reasonable efforts and, when necessary, incur reasonable expenses to limit most uses or disclosures of PHI to the minimum amount necessary to accomplish the purpose of the use or disclosure.

## **12. Do group health plans need formal policies and procedures to guide Minimum Necessary determinations?**

Yes. Group health plans and health care providers must implement policies and procedures that identify people who need access to PHI to do their jobs, identify the types of PHI to which such people need access, limit or control access to those people who need PHI to do their jobs, assign an appropriate person to make Minimum Necessary determinations, and establish rules to guide Minimum Necessary determinations when required on a case-by-case basis.

The people identified as needing access to PHI to do their jobs are referred to as the Plan's administrative workforce.

**13. Are there uses or disclosures of PHI not subject to Minimum Necessary determinations?**

Yes. A Minimum Necessary determination is not required when the PHI is used or disclosed in connection with the participant's treatment OR for disclosures to the participant. The same is true for uses and disclosures made pursuant to participant authorizations.

Finally, Minimum Necessary determinations are not required for disclosures to the U.S. Department of Health and Human Services (HHS) or other government agencies. If a government official requests PHI for official purposes, the group health plan may presume that the requested information is the minimum amount necessary for the stated purpose of the request.

**14. What uses and disclosures may be made by a group health plan without an authorization form?**

Group health plans may use or disclose PHI for treatment, payment, or the management of health care operations.

**15. What is treatment for purposes of the Privacy Rule?**

Treatment includes (1) providing, coordinating, or managing health care and related services for payment by the patient; (2) consultations between health care providers relating to a participant; and (3) participant referrals between health care providers.

**16. What is payment for purposes of the Privacy Rule?**

Payment includes all billing, claims management, reimbursement, and collection activities conducted by, or on behalf of, the group health plan. Payment also includes activities by health plans with respect to premium and benefit payments, as well as eligibility and coverage determinations.

**17. What constitutes management of health plan operations for purposes of the Privacy Rule?**

Health plan operations include all activities related to the group health plan's function as a health care provider, health plan, or health care clearinghouse.

Health care operations include such activities as quality assessment and improvement activities; accreditation, certification, licensing, or credentialing

activities; insurance rating and other insurance underwriting activities; legal, accounting, and audit services; business planning and development activities; and general management, compliance, and administrative activities.

**18. When must group health plans obtain participant authorization to use or disclose PHI?**

The Privacy Rule permits group health plans to use or disclose PHI for purposes other than treatment, payment, or management of health care operations and certain other permitted uses with the participant's written authorization. With proper authorization, disclosures may be made to anyone consistent with the terms of the authorization.

For example, this may occur when: 1) UAW members request the assistance of their UAW Benefits and/or other designated representative to act on their behalf to resolve a claims or other health related matter, or 2) when plan participants request the assistance of a lawyer or other legally recognized designated representative to act on their behalf.

**19. What information must be contained in a written participant authorization?**

Participant authorizations must be written in plain language and must (1) describe the specific PHI to be used or disclosed; (2) identify the person(s) authorized to use or disclose PHI; (3) identify the person(s) or entities to whom the PHI may be disclosed; (4) specify the date or event on which the authorization expires; (5) describe the participant's right to revoke the authorization and the procedure for doing so; (6) state that authorized disclosures may be redisclosed by third parties not subject to the Privacy Rule; and, (7) if signed by a personal representative on the participant's behalf, describe the representative's legal authority.

Authorizations may not be made on an open blanket basis (in order to protect the individual right to choice), however several related claims from the same provider may be chunked together on the same form.

Authorizations are required beginning April 14,2003 for new PHI not yet shared, and are not required retroactively for PHI already shared.

**20. Does an authorization require the signature of the individual whose PHI is to be disclosed?**

Yes. In order for an authorization to be valid under the Privacy Rule, the authorization generally must be signed by the contract holder or dependent who is the subject of the PHI. In the case of an unemancipated minor, the parent or

legal guardian can sign the authorization. An e-mail is acceptable if directly from the contract holder to the Carrier (with cc to the UAW Rep as appropriate).

**21. Will the group health plan require an authorization from a UAW representative acting on behalf of a retired subscriber?**

Yes. An authorization will be required by the group health plan, even if the UAW representative is acting on behalf of a retired subscriber. The authorization must be signed the retired subscriber.

**22. Does the UAW Representative have to retain the Authorization form for the HIPAA required 6-year record retention period in locked files?**

No. The UAW Representative is not a member of the Administrative Workforce and, therefore is not obligated to the 6-year retention requirements. The Carrier is obligated to keep the forms for 6 years. The UAW should follow present confidentiality practices to keep PHI confidential while in your possession and to destroy the confidential materials when no longer needed.

**23. How does a subscriber revoke an authorization permitting PHI to be disclosed to a UAW representative?**

A subscriber may revoke an authorization at any time by providing a written revocation to the benefits service center/ carrier to whom the original authorization was received.

**24. What steps are required by the group health plan to safeguard PHI?**

The Plan must take reasonable steps to ensure that PHI is not intentionally or unintentionally used or disclosed in any manner not consistent with the privacy policies.

Such steps include securing PHI using administrative, physical and electronic access barriers, destroying documents containing PHI that do not need to be retained, training the Plan's workforce members regarding privacy policies, and limiting the persons included as Plan workforce members to those who need PHI to perform their jobs. Physical access to areas containing PHI will be limited, wherever possible, to Plan workforce members only.

**25. What is contained in the Notice of Privacy Practices?**

The employer must notify individuals covered by the group health plan (includes primary plan subscribers, not dependents) of the uses and disclosures of PHI that will be made by the group health plan, the individual's rights and the group health plan's legal duties with respect to PHI.

## **26. When must the Notice of Privacy Practices be provided?**

The Notice must be provided to each covered subscriber at least once before HIPAA's effective date (which is April 14, 2003), and at the time of enrollment for new subscribers. Within 60 days of a material change in the plan's privacy policies, a revised Notice must be provided to all subscribers. A reminder Notice must also be provided every 3 years.

## **27. What rights does a participant have to access, inspect and copy their PHI?**

The health plan must permit a participant or personal representative to inspect and obtain a copy of PHI within a designated record set, except for information compiled in preparation for a legal or administrative proceeding. Upon receipt of a written request by the designated health plan administrator, a health plan must, within 30 days of receiving the request, provide the requested access, provide a written denial notice, or provide written notice that an extension of time is needed to respond to the request.

If the information is maintained by a Business Associate for the health plan, the health plan must instruct the Business Associate to make available the PHI so that the requested access can be provided within the appropriate time frames.

## **28. Can a participant request an amendment of the PHI held by a health plan?**

A participant has the right to request that the health plan amend his PHI. Such a request must be made in writing, submitted to the designated health plan administrator.

## **29. Do participants have a right to an accounting of the disclosures of their PHI?**

A participant has the right to request an accounting of certain health plan disclosures in the six-year period prior to the request, but in no case earlier than April 14, 2003. Each request for an accounting must be submitted in writing to the designated health plan administrator. The accounting must be in writing and include for each disclosure, the date, name of recipient (and address, if known), description of information disclosed and purpose for the disclosure, and a brief statement informing the participant of the basis of the disclosure.

## **30. Does the Privacy Rule allow parents the right to see their children's PHI?**

Yes, the Privacy Rule generally allows a parent to have access to PHI 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. Therefore, if a child is emancipated or has reached the age of majority, parents would not be allowed to see their children's PHI without an authorization. In these cases, the child would be required to sign their own authorization.

In contrast, the Privacy Rule generally requires that the spouse of the individual who is the subject of the PHI obtain an authorization from that individual before the spouse is granted access to the individual's medical records.

**30. Does a health plan have to train members of its workforce on the permissible and impermissible uses or disclosures of PHI?**

The Privacy Rule requires that the plan's workforce members be trained regarding the health plan's policies and procedures related to PHI by HIPAA's effective date, and all new health plan workforce members within a reasonable time. Moreover, a health plan is required to ensure that additional training is provided if one or more of these privacy policies changes in a material way. Such additional training must be delivered within a reasonable time after the change becomes effective.

The UAW Benefits and ESSP Representatives have been educated at the March, 2003 Joint Leadership Conference. Those absent, the Alternates, or newly appointed Reps can access the presentation and audio recording on the UBR site.

**31. Are UAW representatives bound by HIPAA's Privacy Rule?**

Since UAW representatives are not considered part of the Plan's workforce, UAW representatives are not covered under HIPAA's Privacy Rule.

However, while UAW representatives are not covered by the Privacy Rule, if a UAW representative violates the confidentiality of a subscriber's personal health information, it continues to be UAW policy that the UAW representative will be dealt with by the appointing department.

**32. What should a UAW representative do to safeguard the PHI in their possession?**

HIPAA does not change the UAW representatives current safeguarding and confidentiality requirements. However, it is important for each UAW representative to use common sense and those resources available to treat confidential information about others as a UAW representative would want his or her information maintained.

There are a number of ways a UAW representative can safeguard the personal information in their possession. These would include: (1) personal information

should be stored in locked filing cabinets or locked desk drawers, (2) printed material that no longer needs to be retained after use should be shredded or otherwise destroyed, (3) UAW representatives should take reasonable steps to ensure that all incoming faxes and print jobs containing personal information are viewable and retrievable only by the representative, and (4) all electronically-transmitted personal health information should be password protected.

**33. What should a UAW representative do upon discovery that PHI of a subscriber has been inappropriately used or disclosed?**

A UAW representative should address the inappropriate use or should report the potential violation to the Department of Health and Human Services (DHHS) or the Plan's Privacy Officer.

The complaint to the Secretary of the DHHS should be made in writing and generally should be made within 180 days of discovering of the potential violation. Any complaints should be sent to: The U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C. 20201.