



The HIPAA Privacy Rule: Overview and Impact

DISCLAIMER: This information is provided “as is” without any express or implied warranty. It is provided for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney.

A. First Things First: What Is The “HIPAA Privacy Rule”?	1
B. Timeline of HIPAA Privacy Rule	1
C. Overview of the HIPAA Privacy Rule	2
D. How the HIPAA Privacy Rule Impacts WPS	3
E. How the HIPAA Privacy Rule Impacts WPS Customer Service	4
F. Disclosure of PHI to WPS Customers	4
G. How the HIPAA Privacy Rule Impacts the Agents/Agencies with which WPS/EPIC Does Business	5
H. Disclosure of PHI to <u>ASO</u> Group Leaders	5
I. Disclosure of PHI to <u>Risk</u> Group Leaders	6

A. First Things First: What Is The “HIPAA Privacy Rule”?

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) is federal legislation that was passed under the Clinton Administration. Title I of HIPAA has been in effect for several years and deals with health care access, portability, and renewal. Provisions regarding such things as special enrollment rights, creditable coverage, and pre-existing conditions are found in Title I.

Title II of HIPAA, which contains a section entitled “Administrative Simplification,” includes provisions designed to reduce health care costs by standardizing claims processing, as well as provisions designed to improve the privacy and security of health information. As such, the three main parts of the Administrative Simplification provisions are 1) the standards for Transactions and Code Sets; 2) the standards for Privacy of Individually Identifiable Health Information (**the “Privacy Rule”**); and 3) the Security standards.

HIPAA’s Statutory Framework

HIPAA: It’s more than just special enrollment and pre-existing condition exclusion limitations! Here are the several parts of HIPAA and where the Privacy Rule fits in:

- Title I: Health care access, portability, and renewal
- Title II: Preventing healthcare fraud and abuse and Administrative Simplification
 - Subtitle F: *Administrative Simplification*
 - Standards for Electronic Transactions and Code Sets
 - **Privacy Rule**
 - Security Standards
 - Unique Health Identifiers
 - Electronic Signature Standards
- Title III: Tax- related provisions
- Title IV: Group Health Plan requirements
- Title V: Revenue offsets

B. Timeline of HIPAA Privacy Rule

The Privacy Rule has undergone significant changes since it was first proposed in 1999. The U.S. Department of Health and Human Services (“HHS”) issued the final rule on December 28, 2000 after receiving over 50,000



comment letters in response to the proposed rule that was issued November 3, 1999. When the Bush Administration came into office, HHS reopened the regulation for comments and received another 24,000 responses. On April 12, 2001, HHS announced it would move forward with the final regulation but that it would also issue guidance to clarify the Privacy Rule. On July 6, 2001, HHS issued its first set of additional guidance. HHS proposed modifications to the final Rule on March 27, 2002, that significantly changed some of the Rule's requirements. On August 14, 2002, HHS issued final modifications to the Privacy Rule. The compliance date for the HIPAA Privacy Rule is April 14, 2003, for most entities.

Here are the important dates regarding the privacy regulations issued by HHS pursuant to HIPAA:

- November 3, 1999: Proposed Privacy Rule issued
 - December 2000: "Final" Privacy Rule issued by Clinton Administration
 - April 14, 2001: Final Privacy Rule implemented by the Bush Administration
 - July 6, 2001: Guidance on the Final Privacy Rule issued by HHS
 - March 27, 2002: Modifications to the Final Privacy Rule proposed
 - August 14, 2002: Final modifications to the Privacy Rule issued
 - April 14, 2003: Privacy Rule compliance deadline for most entities
 - April 14, 2004: Privacy Rule compliance deadline for "small health plans"
- ❖ *HHS may still issue additional guidance or propose additional changes, before or after the compliance deadline*

C. Overview of the HIPAA Privacy Rule

The HIPAA Privacy Rule establishes in law the basic principle that an individual's health information belongs to the individual and, with several exceptions, that covered entities cannot use the information without permission from that individual.

The HIPAA Privacy Rule applies to "health plans," "health care clearinghouses" and most "health care providers." Collectively, these categories are referred to as "covered entities." For our purposes, the "health plan" category is the most important of the three. Health plans are defined to include health insurers, HMO's, employer-sponsored group health plans, Medicare, Medicaid, and TRICARE, among others.

Several types of benefits are exempt from the HIPAA requirements. For example, information collected in connection with workers' compensation, life, disability, property and casualty, and automobile insurance is not covered by the Privacy Rule. This means that personal health information gathered in the course of offering these benefits is *not* subject to regulation. And any policy, plan or program that offers such benefits is exempt, *but only to the extent that it provides or pays for the cost of such benefits*. Although reinsurance and stop-loss insurance also are excepted benefits, a covered entity's performance of reinsurance-related activities (such as placing stop-loss insurance or handling stop-loss payments for a self-insured plan) is subject to the rules. As a practical matter, however, coverage of such activities is inconsequential, because in most cases use and disclosure of protected health information to perform these activities is permitted without requiring an individual's authorization.

What information does the HIPAA Privacy Rule protect?

The HIPAA Privacy Rule covers Protected Health Information ("PHI"), which is defined broadly to include almost any type of health information that identifies the individual to whom it relates. PHI is health information that 1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and that 2) relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care for an individual.



Examples of PHI could include such types of information as enrollment, eligibility, claims payment, claims status, coordination of benefits, and premium payment, among others. PHI can be created or received in any form or medium (electronic, on paper, oral or otherwise). Health information that has been stripped of individual identifiers, which is referred to as “de-identified information” in the Privacy Rule, does not qualify as PHI and may be used and disclosed freely.

The Privacy Rule includes the following three core requirements:

1. **Use and Disclosure Rules** – Covered entities must obtain specific authorizations for most types of uses or disclosures of PHI *other than* uses and disclosures for treatment, payment, and health care operations. (Most of a covered entity’s uses or disclosures of PHI should fall under these three categories, for which an authorization would not be required.) When authorizations do need to be used, they must be informed and voluntary, and they must meet specific technical requirements. Some public policy exceptions apply. Special rules apply when a group health plan, or its insurer or TPA, shares information with a plan sponsor.
2. **Individual Rights & Privacy Notice** – Individuals will generally be able to access their records and request changes, and they will have the right to receive an accounting of disclosures other than disclosures for treatment, payment, and health care operations, or disclosures made to the individual or pursuant to an authorization. Health plans must provide to individuals a notice of the plan’s privacy practices. When a plan is fully insured, the primary notice obligation is imposed upon the insurer, not the group health plan. Self-funded plans must provide their own notice of privacy practices.

As a result, WPS will issue a HIPAA Notice of Privacy Practices and implement new privacy policies and procedures to provide individuals their access, amendment and accounting of disclosure rights. Covered entities such as WPS must retain documentation showing compliance with rights and title/ office responsible for responding.

3. **Administrative Requirements** – Covered entities must implement written privacy policies and procedures and appropriate safeguards that comply with the Privacy Rule. Specific requirements include designating a privacy official, training employees, establishing a process by which individuals can file complaints, developing a system of sanctions for those who violate the rules, and mitigating harm from such violations.

D. How the HIPAA Privacy Rule Impacts WPS

The Privacy Rule affects the different components of WPS in somewhat different ways. The Rule applies directly to some parts of the company, indirectly to others, and not at all to still others.

WPS Risk (insurance): Health insurers are considered health plans, and thus covered entities, under the Privacy Rule. As a result, this part of our company will need to comply with the full requirements of the Privacy Rule.

WPS’ Self-Funded Employee Group Health Plan: Self-funded employer-sponsored plans are also considered health plans, and thus covered entities, under the Privacy Rule. As a result, our own employees’ plan will need to comply with the full requirements of the Privacy Rule.

WPS Administrative Services: In its capacity as a third-party administrator (TPA) for administrative-services only (ASO) customers, WPS is NOT considered a covered entity. Instead, under the Privacy Rule in such situations, WPS would be considered a “business associate” of the ASO plans that we administer. (The ASO plans themselves would be the covered entities.) Covered entities are required to have “business associate contract” in place with their business associates before disclosing PHI to the business associate, or before allowing the business associate to create or receive PHI on behalf of the covered entity.



WPS TRICARE: Business associate of Health Net Federal Services and of Humana Military Healthcare Services, which in turn are business associates of the Department of Defense TRICARE Management Activity (TMA).

WPS Medicare: Business associate of the Center for Medicare and Medicaid Services (CMS).

EPIC Dental, Vision, Health: Covered entity (health care component) functions.

EPIC Life, Disability: Not covered, either as covered entities or business associate, because these are not “health care components,” as defined by the Privacy Rule.

Looking at WPS, one can see that certain components of our company perform covered entity functions while other components do not. Taken as a whole, WPS and EPIC are considered “affiliated hybrid covered entities.” We are *affiliated* because even though WPS and EPIC are legally distinct corporations, the fact that EPIC is a wholly-owned subsidiary of WPS means that there is common ownership or control. And we are *hybrid* because both WPS and EPIC contain both health care (i.e. covered entity) and non-health care (i.e. non-covered entity) components. Because of their status as affiliated hybrid covered entities, WPS and EPIC are treated as a single entity for purposes of complying with the Privacy Rule.

E. How the HIPAA Privacy Rule Impacts WPS Customer Service

The HIPAA Privacy Rule places limits on the use and disclosure of PHI by covered entities such as WPS. The Rule also requires WPS to verify the identity and authority of those requesting PHI. To this end, WPS is implementing new guidelines to be used by Customer Service and others to explain when, what type of, and to whom PHI may be released. These guidelines will also require that certain pieces of information be gathered from one requesting PHI, such as name, customer number, date of birth and Social Security number, before the PHI may be disclosed or discussed. These verification procedures will help ensure the confidentiality of the PHI of WPS customers.

F. Disclosure of PHI to WPS Customers

Because the Privacy Rule limits how WPS may disclose PHI, our customers will necessarily experience some changes when they contact WPS. The general rule is that adult plan members will be able to call in to discuss their own health information (except diagnosis and procedure codes), but not that of any other family members, except that parents will generally be able to discuss the health information of their minor children on the plan:

- When a customer, spouse, or over-18 dependent contacts WPS regarding their own health information, then after the individual’s identity is verified they will be able to access all of their own information except diagnosis and procedure codes.
- When a participant contacts WPS regarding the health information of their spouse or over-18 dependent, the participant will not be able to access PHI on these people. However, once the participant’s identity is verified, WPS may answer their questions if they first provide to WPS all of the PHI required to answer the questions (for example, claim number, date of service, provider name, etc.). WPS will be able to answer these types of questions because we will not actually be disclosing PHI by doing so. More specific information about their spouse or over-18 dependent would require a written authorization form, which will be available through WPS Customer Service.



- If the parent of a minor dependent, who is on the same WPS/EPIC plan as the dependent, contacts WPS regarding the health information of the minor dependent, then after the parent's identity is verified they will be able to access all of the minor's information except diagnosis and procedure codes. If the parent is not on the same plan as the over-18 dependent, then no health information about the dependent may be disclosed to the parent without documentation of status as personal representative, or verbal consent of parent on the plan.
 - In some situations, federal and/or state laws provide extra protection for health information pertaining to certain "sensitive" claims, such as those for abortion, HIV, sexually transmitted diseases, mental health services, etc. In these situations, a parent will not be able to access health information regarding such claims for their minor child, without an authorization signed by the minor dependent.

Regarding access to health information via the WPS website, all plan members will be able to set up accounts to view their own information but not that of any other family members. Again, there is an exception allowing parents to view the health information of any minor children who may be on the plan.

WPS customers will now enjoy certain individual rights with respect to their health information that is maintained by WPS and used by WPS to make decisions regarding individuals. Included in these are the rights to access PHI, to receive an accounting of certain disclosures of PHI, to request amendment of PHI, and to request confidential communications of PHI.

G. How the HIPAA Privacy Rule Impacts the Agents/Agencies with which WPS/EPIC Does Business

WPS has determined that the Agents/Agencies with which WPS/EPIC has producer agreements are "business associates" of WPS under the Privacy Rule. As a result, WPS is amending its Agency Producer Agreements to contain certain provisions required by the Privacy Rule. These provisions will limit how the Agents/Agencies will be able to use and disclose the PHI of WPS members.

In short, these new privacy amendments will state that each Agency agrees to create, receive, use, or disclose PHI only in a manner that is consistent with the privacy provisions or the HIPAA Privacy Rule, and only in connection with providing the services to WPS/EPIC identified in the WPS or EPIC Agency Producer Agreement. In providing such services to or for WPS/EPIC, the Agency will be permitted, for example, to use and disclose PHI for Payment and Health Care Operations in accordance with the HIPAA Privacy Rule, including but not limited to such customer service activities as assisting a customer with claim, benefits eligibility, and coverage determinations.

If an Agency no longer has a valid Agency Producer Agreement with WPS/EPIC, then WPS will not be releasing PHI *for any reason* to that Agent/Agency without a signed authorization from the individual who is the subject of the PHI.

In addition, WPS will be required to verify the identity of each Agent that requests PHI. For example, before being able to receive PHI from WPS, an Agent will be required to provide certain pieces of information, such as customer name, number, and date of birth or customer address, as well as Agency Tax ID number. If this information cannot be provided, then WPS will not be able to release the PHI.

H. Disclosure of PHI to ASO Group Leaders

In its capacity as a third-party administrator of self-funded group health plans, WPS is a business associate of each such plan it administers. Under the Privacy Rule, neither the group health plan itself, nor its business associates, may disclose PHI to the employer/plan sponsor, unless the plan sponsor has amended its plan



documents to limit how it will use and disclose the PHI. If such amendments have been made and the sponsor certifies to abide by them, then PHI may be disclosed to the sponsor for “plan administration functions.”

WPS is amending the plan documents of its ASO plans to contain the required HIPAA privacy language. Once a plan sponsor has signed these amendments, then PHI may be released to the plan’s group leader to perform the necessary plan administration functions on behalf of the plan. Such functions would include those that fall under the definitions of “payment” and “health care operations” in the HIPAA Privacy Rule, and specifically exclude any employment-related functions.

Since all WPS ASO plans will have their plan documents amended to include the required privacy language, ASO groups should not experience much of a difference in the level of information they receive from WPS, as long as such information will be used for plan administration functions.

I. Disclosure of PHI to Risk Group Leaders

If a group health plan is fully-insured and does not have access to PHI (other than summary health information or plan enrollment/disenrollment information), then the plan’s insurer will be responsible for complying with most of the requirements of the Privacy Rule on the plan’s behalf. Therefore, it is very much in the plan’s interest NOT to have access to PHI.

WPS will generally NOT be disclosing PHI to the group leaders of its fully-insured group health plans. This will allow such groups to avoid most of the Rule’s requirements, as these requirements will be met by WPS. However, if an employee/participant of such a plan wishes to allow the group leader to have access to their PHI to assist with a claim dispute or other matter, then the employee would be required to sign a detailed authorization stating this. WPS would then only disclose the PHI to the group leader in accordance with the signed authorization.

In situations where a risk group leader contacts WPS on behalf of one of their employees and volunteers all of the relevant pieces of PHI necessary to address an inquiry, then WPS will be able to answer questions directly relevant to that inquiry, as long as those answers do not result in the disclosure of PHI by WPS. In such situations, no authorization from the individual would be required, since WPS would not be considered to be “disclosing” PHI to the group leader.