

## **FREQUENTLY ASKED QUESTIONS ABOUT SELF-FUNDED GROUP HEALTH PLAN HIPAA PRIVACY RULES**

- Q.1. When is the Privacy Law Effective?
- A.1. April 14, 2003 for plans with \$5 million or more in claims during the prior year and April 14, 2004 for plans with less than \$5 million in claims. (Self-funded plans that adjudicate their own claims and have less than 50 participants do not have to comply with the Privacy law.)
- Q.2. Is there an exemption for government and church plans?
- A.2. No. Unlike ERISA, this Rule applies to government and church plans.
- Q.3. What kinds of plans must follow the Privacy law?
- A.3. Insured and self-funded group medical, dental, vision, prescription drug and health flexible spending account plans must comply. Depending on how they are set up, wellness programs and EAP's may need to comply. HMO's, Medicare and Medicaid also must comply.
- Disability income, life insurance and automobile insurance plans are exempt. Workers compensation is not subject to the law either.
- Q.4. What is a Covered Entity?
- A.4. A Covered Entity is a health plan (which includes medical, dental, vision, and prescription drug plans and health FSA's), a health care clearinghouse or a health care provider.
- Q.5. What is a Business Associate?
- A.5. A Business Associate is a person or firm that performs a function for a Covered Entity. Business Associates include TPA's, brokers, pharmacy benefit managers and utilization review companies.
- Q.6. Is a reinsurer/stop loss carrier or MGU a Business Associate of the plan?
- A.6. No, reinsurers, stop loss carriers and MGU's are not considered Business Associates because the carrier simply provides reimbursement.
- Q.7. Is enrollment information covered by this law?
- A.7. No, it is not. Sponsors may freely obtain and provide enrollment and disenrollment information from and to the health plan.
- Q.8. What is "PTO"?
- A.8. "PTO" stands for Payment, Treatment and Operations. Covered Entities may use protected health information for Payment, Treatment and Operations without authorization or consent from the individual, as long as:
1. The use is disclosed in the entity's Notice of Privacy Practices; and
  2. The information requested or disclosed is the "minimum necessary" to complete the function.

Q.9. What is “PHI”?

A.9. “PHI” is short for “protected health information”. Protected health information is individually identifiable health information that:

1. Relates to the physical or mental health of an individual, the provision of health care to an individual (including insurance processes, quality assessment, case management, and disease and disability management activities), or the payment for the provision of health care to an individual (including claims processing, utilization review, and coordination of benefits);
2. Is created or received by a health care provider, health plan, or health care clearinghouse; and
3. Identifies the individual, or there is a reasonable basis to believe the information can be used to identify the individual.

Q.10. What is “Payment”?

A.10. “Payment” includes any information needed to determine the plan’s responsibility to provide a benefit, and includes:

1. Eligibility determination;
2. Adjudicating benefits;
3. Coordination of benefits;
4. Subrogation of claims;
5. Billing and collection activities;
6. Claims management;
7. Obtaining stop loss or similar insurance payments;
8. Medical necessity determinations;
9. Determinations regarding appropriateness of care, coverage or justification of charges;
10. Utilization review, including
  - Pre-certification;
  - Preauthorization of services;
  - Concurrent review;
  - Retrospective review;
11. Issuing claims payments.

Q.11. What is “Treatment”?

A.11. “Treatment” means the provision, coordination or management of health care and related services by health care providers including consultations and referrals.

Health plans are rarely involved in “Treatment”.

Q.12. What are “Health Care Operations”?

A.12. Health Care Operations are activities needed to manage the Plan or provision of health care. They include:

1. Conducting quality assessment and improvement activities, and related functions;
2. Population based activities relating to improving health or reduce health care costs;

3. Development of protocols;
4. Case management and coordination of care;
5. Contacting health care providers and patients with information about treatment alternatives;
6. Reviewing competence or qualifications of health care professionals;
7. Underwriting, premium rating, etc., related to placing or reviewing contracts for health insurance, health benefits or stop loss or reinsurance coverage;
8. Medical review, legal services and audit functions, including fraud and abuse detection or compliance programs;
9. Business planning and development, including
  - Cost management
  - Formulary development and administration;
  - Development or improvement of payment methods or coverage policies;
10. Business management and general administrative activities, such as
  - Resolution of internal grievances;
  - Due diligence in connection with sale or transfer of a business that involves transfer of a health care plan.

Q.13. What is “minimum necessary”?

A.13. “Minimum necessary” is similar to “need to know”. This law is not intended to prohibit all disclosure of PHI, but to limit it as much as reasonably possible.

When deciding if the data is the minimum necessary amount, you should consider:

1. What function needs to be performed?
2. Who needs to be involved to efficiently perform the function?
3. Is there a method that uses less PHI than the current method?

For example, does the Controller need to know the name of the patient to authorize a check? What about the diagnosis? Different plans will answer this question differently.

Q.14. Is there any time that “minimum necessary” does not apply?

A.14. The “minimum necessary” standard does not apply to inquiries from the Covered Person or sharing information with a person the Covered Person has authorized disclosure to.

Q.15. What happens if a provider, plan representative or business associate requests more information than we think is the minimum necessary data?

A.15. If the requester represents (preferably in writing) that the information is the minimum necessary for the stated purpose, the requested information may be released to that person. Unless the request is **clearly** unreasonable and excessive, the requested information should be disclosed.

Q.16. Can the plan sponsor staff help resolve claim issues under HIPAA?

A.16. The plan sponsor can access protected health information for treatment, payment, and health care operations purposes if the needed paperwork plan amendment and certificate is in place. As it is questionable whether the plan

sponsor needs to assist with claims issues to manage the plan, we recommend an authorization be obtained from the covered person.

If you believe this practice does meet “minimum necessary” you should add it to your Notice of Privacy Practices.

In that case, the information shared with the plan sponsor needs to be the minimum amount of covered person information needed to complete the specific task. In this example, a plan sponsor resolving a specific claim may need some details about that claim to perform the function, but information about previous claims need not be shared.

Q.17. Will reports that are shared today with the plan, plan sponsor, or broker change as a result of HIPAA?

A.17. Nyhart will de-identify or strip reports that we send out of any PHI if we believe that this information exceeds minimum necessary. (For example, if a report contains the patient’s social security number, diagnosis, address, etc., this information will be “blocked out” on the report or listed as “not authorized to view”.)

These reports will now be de-identified:

- CVA – Claim Void Audit Trail;
- ISA – Individual Specific Analysis;
- RMC – Monthly Check Register;
- RMW – End of Month Paid Claims Register.

If you advise us in writing that identified information is minimally necessary for some or all of these reports, we will provide the full data to you.

Q.18. Is there a way to avoid having to follow this law?

A.18. Yes, if the health plan does not see any PHI (protected health information) except for summary information it does not have any PHI to protect. This may be an option for fully insured plans and some health FSA’s.

Q.19. What is summary information?

A.19. Summary information is claims data from which all PHI has been removed. All of these items are considered PHI:

1. Names;
2. All geographic subdivisions smaller than a 5 digit zip code,
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;

5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Q.20. Can Social Security Numbers be utilized to identify participants?

A.20. In most cases, yes. The privacy regulation does not prohibit the use of Social Security Numbers (SSN) as a member identifier. Additionally, the federal unique health identifier regulation has not made progress on a national replacement of the SSN. However, there is a state law in California that will soon prohibit the use of SSN as an identifier to access services, such as health care services, for participants who live in California.

Q.21. Who is responsible for enforcing this law?

A.21. The federal agency responsible for enforcement is the Department of Health and Human Services ("HHS).

Q.22. What happens if I can't or don't follow this law?

A.22. Currently HHS is only investigating complaints, and not performing independent audits. If they receive a complaint and the Covered Entity promptly corrects the problem, penalties will not be assessed.

Refusals to follow the law will be referred to the Department of Justice. Potential penalties are severe:

- Non-criminal violations (including disclosures made in error) –penalties of \$100 per violation up to \$25,000 per year, per standard violated;
- Criminal violations (done knowingly) for obtaining or disclosing protected health information – up to \$50,000 and one year in prison, but for doing

so under “false pretenses,” up to \$100,000 and five years in prison, and for intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm, up to \$250,000 and ten years in prison;

- Patients may not sue in federal court for medical privacy violations. However, individuals may report privacy violations to the HHS’ Office of Civil Rights. If there is a violation of the privacy terms of a group health plan, a federal suit under ERISA is possible.

Q.23. Where can I get more information about this law?

A.23. The federal government has 2 helpful websites, at:

[www.cms.gov/hipaa/Administrative](http://www.cms.gov/hipaa/Administrative) Simplification;  
[www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa)

There is also a good private site at:

[www.hipaadvisory.com](http://www.hipaadvisory.com)

9/20/04