

HIPAA Privacy

What Medical Information May A Plan Sponsor Access?

Employers providing group medical insurance to their employees are plan "sponsors." The "plan" is managed and insured by the carrier. As long as the plan sponsor (employer) takes "hands off" approach to "personal health information" (PHI), the HIPAA privacy requirements will apply only to the "plan" and the carrier will take care of compliance. But, does taking a "hands off" approach to avoid the cost of HIPAA compliance deny an employer access information needed to handle plan administration matters and evaluate insurance proposals?

The answer is "NO!" Employees can reveal any or all their PHI to their employer--as long as there is no coercion or intimidation. In fact, some laws like FMLA and those related to workers' compensation require it. HIPAA also provides employers the opportunity to access PHI when the information and its use is limited by a signed authorization. And, even if your business does not want to comply with HIPAA privacy regulations, there is a lot of information you will need for group medical plan selection and management that you can access. The HIPAA regulations specifically permit the following information to be given to the employer ("sponsor") without invoking major compliance requirements for the employer:

1. De-identified information. If 18 specific identifiers are removed or if it is part of a professional statistical analysis—"sponsors" (employers) can receive PHI from the "plan" (carrier). (See attached list of 18 identifiers).
2. Enrollment/dis-enrollment information. The plan can disclose whether an individual is enrolled and the plan that they have selected specifically for enrollment and dis-enrollment purposes.
3. Summary health information. Summary premium, claims and large claims information may be disclosed to the sponsor (employer) for the purposes of obtaining premium bids or modifying or terminating the plan (this information can include the participant's zip code).

While HIPAA does severely restrict access to PHI by sponsors (employers) who choose to avoid compliance with complicated regulatory requirements, HIPAA does permit access to de-identified information sufficient to carry out most of the important functions sponsors must perform. The HIPAA privacy rules were not intended to permit carriers to establish a monopoly over employers by denying them access to critical "personal health information."

Please remember: These notes do not represent financial, legal, or tax advice but they do represent our view of 45 CFR 164.504, 531 and similar provisions.

How PHI Becomes "De-identified"

Most PHI ("personal health information") can be released by the plan to the Sponsor if the plan removes the following 18 identifiers:

1. Names
2. Sub-state geographic subdivisions aggregated to the 5-digit ZIP
3. All elements of dates (except year) if the dates related to AN individual (with exceptions)
4. Telephone numbers
5. Fax numbers
6. E-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/license plate numbers
13. Device identifiers and serial numbers
14. URLs (Web addresses)
15. IP (Web location) addresses
16. Biometric identifiers, including finger and voiceprints
17. Full face photos and any comparable images
18. Other unique identifying number, characteristic, or code

None of these identifier deletions prohibits a plan/carrier from providing summary premium, claims or even claims by broad diagnostic categories and amounts of large claims as long as individual participants cannot be identified from the data.

3/2003

Benefit Innovations, Inc.

How PHI Becomes "De-identified"

Most PHI ("personal health information") can be released by the plan to the Sponsor if the plan removes the following 18 identifiers:

1. Names
2. Sub-state geographic subdivisions aggregated to the 5-digit ZIP
3. All elements of dates (except year) if the dates related to AN individual (with exceptions)
4. Telephone numbers
5. Fax numbers
6. E-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/license plate numbers
13. Device identifiers and serial numbers
14. URLs (Web addresses)
15. IP (Web location) addresses
16. Biometric identifiers, including finger and voiceprints
17. Full face photos and any comparable images
18. Other unique identifying number, characteristic, or code

None of these identifier deletions prohibits a plan/carrier from providing summary premium, claims or even claims by broad diagnostic categories and amounts of large claims as long as individual participants cannot be identified from the data.

3/2003

Benefit Innovations, Inc.