
SOCIETY OF ACTUARIES

Article from:

# Health Section News

April 2001 – Issue No. 40

# *Actuarial and Underwriting Implications of the Final Health Privacy Rule*

***by Rowen B. Bell***

**EDITORIAL NOTE:** *Shortly before this issue went to print, it was announced that the purportedly final federal health privacy rule discussed in the article below was being reopened for additional public comment. Consequently, some of the interpretations made in this article may no longer be applicable after the rule has been reshaped. An update of this article will be provided once the privacy rule reaches its ultimate form.*

In December 2000, the Department of Health and Human Services published its final rule on "Standards for Privacy of Individually Identifiable Health Information." Companies will need to attain compliance with this rule, which is the second of the HIPAA "administrative simplification" regulations to be published in final form by February 26, 2003.

This final rule supplants the proposed rule, which had been exposed for public comment in November 1999. The proposed rule contained several ambiguities that created significant interpretative questions as to how the rule would impact actuarial and underwriting processes.

The final rule achieves greater specificity on these issues, with many of the open questions having been recognized by HHS, thanks in part to comment letters submitted on the proposed rule by insurers and insurance trade organizations.

The intent of this educational article is to provide a brief overview of the final privacy rule followed by a discussion, organized topically, of its implications for actuarial and underwriting functions. Please note that any opinions expressed herein are merely the author's interpretations and should not be considered definitive. The privacy rule is a highly complex subject, and any organization should consult legal counsel to gain an appropriate understanding of how it will be impacted by the rule.

## What is the scope of the privacy rule?

The principal subject of the privacy rule is "individually identifiable health information," or "IIHI." The passage below is an excerpt from the definition of IIHI [§164.501] highlighting the aspects of greatest relevance to health actuaries:

> *"[IIHI includes] … information that is created or received by a health plan … and relates to … the past, present, or future payment for the provision of health care to an individual … and with respect to which there is a reasonable basis to believe the information can be used to identify the individual."*

For example, a listing of paid claims by claimant where the claimant is identified by name or by social security number would qualify as IIHI.

The phrase "health plan" has a specific meaning here. An insurer would only be considered a "covered entity" to which the privacy rule applies insofar as it is performing activities that fall under the definition of "health plan." As a result, some portions of a health insurer's business may be subject to the privacy rule while other portions are not.

Most notably, an issuer of an insured medical, Medicare Supplement, Medicare+Choice, dental, or long-term care contract would be considered a "health plan," and thus the privacy rule would apply directly to such operations.

However, an insurer would not be considered a "health plan" with respect to its activities as: an issuer of stop-loss, disability income, accident-only, life insurance, or workers compensation contracts; as a reinsurer of medical or long-term-care business; or as an administrator of medical business under ASO contracts. Therefore, it would not be considered a "covered entity" subject to the privacy rule with respect to health information arising from such activities. Nonetheless, it may still be impacted by the privacy rule under the "business associate" provisions when acting as a reinsurer or administrator of medical business, as we discuss below.

## What is the main thrust of the privacy rule?

The privacy rule prevents covered entities from using or disclosing individually identifiable health information except under certain circumstances delineated within the rule, the most notable of which is the following:

> *"A covered entity is permitted to use or disclose [IIHI] … pursuant to and in compliance with a consent that complies with §164.506, to carry out treatment, payment, or health care operations." [§164.502(a)(1)(ii)]*

The terms "use," "disclose," "treatment," "payment," and "health care operations" are given explicit definitions in the privacy rule. Later, we shall discuss specific situations where these definitions govern what one can and cannot do with IIHI under the privacy rule.

*(continued on page 6)*

## *Actuarial and Underwriting Implications of the Final Health Privacy Rule*

*continued from page 5*

The phrase "pursuant to and in compliance with a consent that complies with §164.506" should, in practice, have little impact for health insurers. To wit: An insurer may, but is not obliged to, seek consent from its enrollees to use their IIHI for purposes of payment or health care operations [§160.506(a)(4)]. If the insurer decides to seek such consent, then it is allowed to make each enrollee provide that consent as a condition of enrollment [§160.506(b)(2)].

The consent must state that the enrollee has the right to request that the insurer restrict its use of his/her IIHI; however, the insurer does not have to agree to any requested restrictions, although if it were to agree then it would be bound by the agreed-upon restrictions [§160.506(c)(4)]. In short, an enrollee should not be in a position to unilaterally prevent the insurer from making use of his/her IIHI in a way normally permissible under the privacy rule.

### What are some of the other important concepts in the privacy rule?

There are three other concepts in the privacy rule that one should be familiar with: "business associate," "de-identified information," and the "minimum necessary" standard.

*Business Associates*

An entity subject to the privacy rule (e.g., an insurer or a self-insured group health plan) might want a third party to perform certain essential business functions requiring that third party to have access to IIHI. Examples of this would include the following:

- An insurer hiring a TPA to process claims
- An insurer hiring an MGU to perform underwriting and enrollment functions
- An insurer hiring a consultancy to perform actuarial work
- An insurer ceding risk to a reinsurer
- A self-funded group hiring an insurer to perform administrative services
- A self-funded group ceding risk via stop-loss insurance to an insurer

In recognition of the existence of such business arrangements, the privacy rule defines a "business associate" as someone who either: performs certain specified functions involving the use or disclosure of IIHI on behalf of the covered entity: or provides certain specified services to the covered entity necessitating the receipt of IIHI from the covered entity [§160.103]. In each of the previous examples the third party would be considered a "business associate" of the covered entity.

Business associates are not directly subject to the privacy rule. Rather, the rule requires the covered entity to insert privacy-related clauses into its contracts with business associates and prevents it from having business associates do anything that the privacy rule would forbid the covered entity from doing itself:

> *"A contract between the covered entity and a business associate must establish the permitted and required uses and disclosures of [IIHI] by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate [the privacy rule] if done by the covered entity, except that [the business associate may] use and disclose [IIHI] for the proper management and administration of the business associate..." [§164.504(e)(2)(i)]*

***"Business associates are not directly subject to the privacy rule. Rather, the rule requires the covered entity to insert privacy-related clauses into its contracts with business associates and prevents it from having business associates do anything that the privacy rule would forbid the covered entity from doing itself."***

*De-identified Information*

In theory, one could "de-identify" individually identifiable health information by stripping away those pieces of data that could be used to identify the individuals involved. Once IIHI has been sufficiently de-identified through such a process, the remaining information could be used and distributed without raising privacy concerns. However, the framers of the privacy rule were faced with the following dilemma: how much information needs to be removed or masked before there is no longer a "reasonable basis" to believe that the information remaining could be used to identify the individuals?

Under the privacy rule, in order for health information to be considered as

having been de-identified, one of two alternative conditions must be satisfied.

The first alternative is that "a person with appropriate knowledge of and expertise with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable … determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information … to identify … [the] subject of the information" [§164.514(b)(1)].

The second alternative is that a prescribed list of data elements must be removed or encrypted:

> *"The following identifiers of the individual or of relatives, employers, or household members of the individual, must be removed:*
> *(A) Names;*
> *(B) All geographic subdivisions smaller than a State, including … zip code … except for the initial three digits of a zip code if … the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people … ;*
> *(C) All elements of dates (except year) for dates … including birth date, [and] admission date … ; …*
> *(G) Social security numbers; …*
> *(I) Health plan beneficiary numbers;*
> *(J) Account numbers;*
> *(K) Certificate/license numbers; …" [§164.514(b)(2)(i)]*

While the passage above refers only to removal, a later clause indicates that encryption is equally acceptable, so long as the decryption key (if retained) is kept secret [§164.514(c)(2)], thus preventing the user of the de-identified data from reconstructing the individual identifiers.

*Minimum Necessary Standard*

While the privacy rule permits the use or disclosure of IIHI in certain circumstances, at the same time it places burdens on entities to ensure that such use or disclosure is minimized:

> *"When using or disclosing [IIHI] or when requesting [IIHI] from another covered entity, a covered entity must make reasonable efforts to limit [IIHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." [§164.502(b)(1)]*

The rule clarifies an entity's responsibilities in adhering to this "minimum necessary" standard:

> *"A covered entity must identify those persons … in its workforce who need access to [IIHI] to carry out their duties, and for each such person … [the entity must identify] the categories of [IIHI] to which access is needed and any conditions appropriate to such access … A covered entity must make reasonable efforts to limit the access of such persons … to [IIHI] consistent with [the categories to which access is needed]." [§164.514(d)(2)]*

Similar clauses apply to an entity's disclosures of IIHI and to an entity's requests for IIHI from another covered entity.

## How does the privacy rule affect underwriting of new cases?

We have already mentioned that IIHI may be used or disclosed by a covered entity for the purposes of "health care operations" (or "HCO"). The definition of HCO [§164.501] contains many clauses, the most important of which from the health insurer's standpoint is clause (3):

> *"[HCO includes] underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance) …"*

Thus, the final privacy rule explicitly permits a prospective client to disclose, and an insurer to use, IIHI in order to design and price an insurance product for that client. This is a significant improvement over the proposed privacy rule, which would have explicitly prevented a prospective client from disclosing IIHI to an insurer for underwriting or rating purposes prior to its becoming a client of that insurer.

The final privacy rule does stipulate that an insurer who receives IIHI in order to underwrite a prospective client cannot use or disclose that information for any other purpose in the event that the client does not enter into an insurance contract with the insurer [§164.514(g)].

It is also worth noting that the privacy rule would force a health care provider to obtain explicit authorization from an individual in order to disclose that individual's health information to an insurer for purposes of pre-enrollment underwriting. Of course, if the individual refuses to authorize the provider to disclose the information requested by the insurer, then the insurer has the right to refuse to enroll the individual [§164.508(b)(4)(ii)(A)].

## How does the privacy rule affect underwriting of renewal cases?

As noted above, clause (3) of the HCO definition incorporates underwriting and rating for renewal business, and hence the use of IIHI for such purposes is permitted.

*(continued on page 8)*

## *Actuarial and Underwriting Implications of the Final Health Privacy Rule*

*continued from page 7*

Note that clause (3) also addresses policy replacement, which may be of particular importance in the individual market. The proposed privacy rule did not mention policy replacement and thus raised questions as to whether an insurer would be permitted to take policyholder experience into account in underwriting or pricing for a replacement policy form; the final privacy rule places no new restrictions on doing so.

However, in order to comply with the privacy rule's minimum necessary standard, the insurer may need to adopt new procedures regarding the internal use of health information by its underwriting department. The following illustration appears in the preamble to the privacy rule:

> *"For example … a health plan could permit its underwriting analysts unrestricted access to aggregate claims information for rate setting purposes, but require documented approval from its department manager to obtain specific identifiable claims records for the purpose of determining the cause of unexpected claims that could influence renewal premium rate setting." [Preamble, p. 82544]*

If underwriting is outsourced to an unrelated company (e.g. an MGU), then that company is considered a "business associate" of the insurer, and the contract between the two companies will need to address certain issues related to the use and disclosure of IIHI, as discussed earlier.

### How does the privacy rule affect the disclosure to a group of its own experience?

There are two separate issues here: the disclosure of IIHI to the group; and the use of IIHI by the insurer to create non-IIHI exhibits for the group.

The main problem with respect to the first issue, as perceived by the framers of the privacy rule, is how to strike a balance between the plan sponsor's legitimate need for certain pieces of health information versus the desire to prevent health information from being used by the plan sponsor for employment-related purposes.

To that end, the privacy rule focuses on the relationship between the group health plan (not the insurer, but rather the group's benefit program) and that plan's sponsor (the employer itself). However, there are two distinct circumstances in which the rule discusses the insurer's role. The first is that the insurer can disclose "summary health information" to the plan sponsor to allow the sponsor to solicit premium quotes or to facilitate the sponsor's efforts to modify, amend, or terminate the health plan [§164.504 (f)(1)(ii)]. The definition of "summary health information" is as follows:

> *"… information, which may be [IIHI], and that summarizes the claims history, claims expenses, or types of claims experienced by individuals for whom the plan sponsor has provided benefits under a group health plan, and from which the information described at §164.514(b)(2)(i) has been deleted, except that … geographic information … need only be aggregated to the level of a five digit zip code." [§164.504(a)]*

The "information described at §164. 514(b)(2)(i)" appears earlier in this article, in the section on de-identified information. Thus, it would appear that the summary claims information disclosed to the sponsor could include a listing of paid claims by claimant where the claimant was identified only by birth year, gender, and five digit zip code (and not by name or SSN).

The second circumstance embedded in the rule involves the plan sponsor's need for IIHI in order to perform administrative functions relating to the group health plan:

> *"[§164.504(f)] permits group health plans … to authorize health insurance issuers … to disclose [IIHI] to plan sponsors if the plan sponsors voluntarily agree to use and disclose the information only … for plan administration functions performed on behalf of the group health plan …" [Preamble, p. 82508]*

Procedurally, the plan sponsor will need to make certain specified amendments to its plan documents and will need to certify to the group health plan that those amendments have been made [§164.504(f)(2)]. (For example, one of the required amendments states that the plan sponsor will not use or disclose such information for employment-related actions.) Once the insurer has received this certification, it may disclose the necessary IIHI to the plan sponsor. This approach was designed to minimize the obligations of the insurer with respect to such disclosures:

> *"We have included this certification requirement … to reduce the burden on [health insurers]. Without a certification, [health insurers] would need to review the plan documents in order to ensure that the amendments have been made before they could disclose [IIHI] to plan sponsors. … The receipt of the certification … is sufficient basis for the [health*

*insurer] to disclose [IIHI] to the plan sponsor." [Preamble, p. 82508].*

Returning now to the second issue, clause (6)(ii) of the HCO definition states that HCO includes "customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that [IIHI] is not disclosed …". Thus, the privacy rule preserves the insurer's ability to use IIHI to prepare exhibits for customers, so long as IIHI is not actually contained in such exhibits. The preamble to the rule provides some examples of the types of "data analyses" contemplated by this clause:

- "… a plan sponsor may want to understand why its costs are rising faster than average;"
- "… a plan sponsor may want to understand … why utilization in one plant location is different than in another location;"
- "… an association that sponsors an insurance plan for its members may want information on the relative costs of its plan in different areas." [Preamble, p. 82491]

The rule also anticipates that different insurers may need to cooperate in preparing such exhibits for a common client:

*"… when a plan sponsor has several different group health plans, or when such plans provide insurance or coverage through more than one health insurance issuer or HMO, the covered entities may jointly engage in this type of analysis …" [Preamble, p. 82491].*

## How does the privacy rule affect ratemaking and reserving?

As mentioned earlier, "premium rating" is included in clause (3) of the HCO definition. There is every reason to believe that this phrase is meant to permit the use of IIHI for both the general (creating the manual rates) and specific (modifying those rates for a particular policy) aspects of the ratemaking function.

Clause (6) of the HCO definition states that HCO includes "business management and general administrative activities of the entity." The preamble clarifies that this clause is intended to include all "general administrative and business functions necessary for the covered entity to remain a viable business" [Preamble, p.82490]. Reserving, and any other financial reporting functions requiring the internal use of IIHI, can be presumed to fall into this category. While the privacy rule preserves the right of an insurer's actuaries to make internal use of IIHI for ratemaking or reserving, it may also require changes in business practices regarding actuaries' access to claims information.

For example, it is not uncommon today for an employee of a health insurer's actuarial department to have complete access to a database of enrollees' claims payments, where that database contains individual identifiers such as names or social security numbers. However, since the vast majority of that employee's work would not require the employee to need to know the identity of the claimants, this unlimited access would violate the privacy rule's "minimum necessary" standard.

Here is an outline of one possible approach to this problem. The insurer could establish a "dual" of the claims database, containing the same information but with many of the individual identifiers removed (e.g., names) or encrypted (e.g., social security numbers). The encryption algorithm should be retained, so that comparisons can be made between the dual and original databases, but it should be kept guarded. The creation of the dual database would be a batch job run nightly, so that its information is as up-to-date as that in the original database.

The actuarial department would be given unlimited access to the dual database, which would suffice for most situations. For certain specified purposes, access to the original database would be permissible; an example here would be reserving for large claims, where the actuary would need to know the claimant's identity in order to converse with case management personnel as part of the reserving process.

Note that this dual database would not need to consist of "de-identified information" in the sense defined in the privacy rule. It could contain items necessary for actuarial work that do not meet the de-identification standard, such as actual admission dates, group identifiers, and five digit zip codes. The key point is that this two-database structure would provide the actuarial department with the information needed to perform its work while limiting the potential for privacy violations.

***"While the privacy rule preserves the right of an insurer's actuaries to make internal use of IIHI for ratemaking or reserving, it may also require changes in business practices regarding actuaries' access to claims information."***

If the insurer subcontracts ratemaking or reserving to an actuarial consultant, then the insurer would be allowed to disclose IIHI to the consultant for that purpose, and in this case, the consultant becomes a "business associate" of the insurer, as evidenced by this excerpt from the definition thereof [§160.103]:

*"[Business associate includes] a person who … provides, other than in the capacity of a member of the workforce of such covered entity,*

*(continued on page 10)*

## *Actuarial and Underwriting Implications of the Final Health Privacy Rule*

*continued from page 9*

> *… actuarial … services to or for such covered entity … where the provision of the service involves the disclosure of [IIHI] from such covered entity … to the person."*

Again, the minimum necessary standard would apply with respect to the disclosure of IIHI to the consultant. If the consultant's work can be performed using strictly de-identified information, then that is the preferred route, since doing so would not create a business associate relationship.

Otherwise, the insurer can rely on the consultant's representation that the information requested is the minimum necessary for the stated purpose [§164.514(d)(3)(iii)(C)].

### How does the privacy rule affect reinsurance?

The final privacy rule clarifies that reinsurers, and also stop-loss insurers, are not covered entities and thus are not directly subject to the privacy rule.

If an insurer assumes risk from a covered entity under a reinsurance contract, then it is considered a business associate of the ceding carrier. (Note that this applies to medical, dental, or long-term care reinsurance assumed, but not to disability income or workers' compensation, since those latter lines of business are excluded from the scope of the privacy rule.)

The ceding carrier is allowed to disclose IIHI to the insurer for underwriting or rating purposes, but the reinsurance contract needs to specify what information will be disclosed and under what circumstances. The insurer may use the IIHI received from the ceding carrier for its own business purposes, such as reserving, and it can further disclose that IIHI if necessary for that purpose (e.g., if it hires a consultant to set the reserves on the assumed business).

The above comments apply equally to an insurer issuing stop-loss insurance to a self-funded group health plan; the insurer is a business associate of the group, not a covered entity, and its contract with the group needs to address the insurer's use and disclosure of IIHI.

If an insurer instead cedes risk under a reinsurance contract, then as noted earlier, the reinsurer is a business associate. Also, the act of "obtaining payment under a contract for reinsurance" is specifically mentioned in the privacy rule definition of "payment" [§164.501], and thus the use or disclosure of IIHI for such purposes is permitted, subject as always to the minimum necessary standard.

### How does the privacy rule affect the performance of due diligence for acquisitions?

Clause (6)(iv) of the HCO definition reads as follows:

> *"[HCO includes] due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity."*

The preamble clarifies that this clause is intended to include sales, mergers, acquisitions, and consolidations involving all of, or just a division of, a covered entity. Thus, it is sufficiently broad to permit the disclosure of IIHI to, and use thereof by, potential buyers in virtually any M&A activity involving two health insurance entities. This wording did not exist in the proposed privacy rule.

Of course, the seller is bound by the minimum necessary standard in determining which information is to be disclosed for due diligence purposes:

> *"[For any disclosure not made on a routine or recurring basis] a covered entity must develop criteria designed to limit the [IIHI] disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought." [§164.514 (d)(3)(ii)(A)]*

This might imply, for instance, that any policy or claims listings provided to prospective buyers should contain encrypted social security numbers rather than actual ones.

*Rowen B. Bell, FSA, MAAA, is an associate actuary at Blue Cross/Blue Shield Association in Chicago. He can be reached at* rowen.bell@bcbsa.com.