INDEPENDENT INSURANCE AGENTS & BROKERS OF LOUISIANA
9818 BLUEBONNET BLVD.
BATON ROUGE, LA 70810
P: 225/819-8007 F:225/819-8027
www.iial.com

Technical Advisory

TA-222 **APRIL 30, 2003**

SUBJECT: HIPAA and Independent Agents

BACKGROUND: The "Information Age" has brought sweeping changes to the modern world. Most have been beneficial, but some have created enormous and sometimes frightening problems. One of the greatest casualties has been privacy of personal information. As a result, several federal privacy laws have been enacted in recent years, including the Fair Credit Reporting Act (FCRA), the Driver's Privacy Protection Act (DPPA), and the Gramm-Leach-Bliley Act (GLBA), all of which impact the insurance industry.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed, with myriad provisions relating to a broad spectrum of health insurance issues, including protecting the privacy of health information.

The law stipulated that Congress enact specific provisions for privacy standards relating to personal health information within three years. The 1996 law further provided that should Congress fail to pass such subsequent legislation on health information privacy, the U. S. Department of Health and Human Services (HHS) would be required to implement such privacy standards.

Congress did not pass the required legislation relating to privacy standards within the three-year time frame, so in 1999, HHS made its initial proposals for protecting personal health information. These proposals generated over 52,000 public comments. After a lengthy review process, HHS released its initial administrative rules in December, 2000.

In March, 2001, HHS requested additional public comments on the rules, and received another 11,000 public comments. Revised rules were issued in March, 2002. Final rules were issued August 14, 2002, with an effective date of April 14, 2003. Within HHS, the Office of Civil Rights (OCR) has the responsibility for implementing and enforcing the privacy rule.

The huge volume of public comments, and the subsequent revisions to the privacy rules, reflect just how complicated the issue of health information privacy is. In the

HHS/OCR "Summary of the HIPAA Privacy Rule" released this month, the introductory statement reflects the tortuous rule-making journey:

"*A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed."*

In fact, even after the effective date of the rule, much is not known about many operational details. Many articles from a wide variety of sources complain about the complexity, or vagueness, of many facets of the rule. That is probably an unintended outcome to rules that are "flexible and comprehensive."

Implementation of the rule is taking many forms, from the mundane to the complex. Health care providers are advising the staff to shut the covers of chart holder bins near patient beds. Information boards at nursing stations and other locations inside treatment areas are being concealed or moved from the view of visitors or other patients. Pharmacies are putting customer receipts inside bags, rather than attaching them to the outside. Hospitals are reviewing their procedures for how flowers are delivered to patients, and which family members of patients can receive medical information and progress reports.

On the complex side, entities covered by HIPAA are mailing privacy notices, having authorization forms signed, designing and implementing privacy rules for administration, automation, and communication. Larger organizations have budgeted millions of dollars for HIPAA compliance. In an ironic twist only a bureaucrat could love, the HIPAA rules refer to many of these procedures as "administrative simplification."

MAIN POINTS: Probably the best reference point for understanding HIPAA is the GLBA – the Gramm-Leach-Bliley Act, which all agencies had to comply with starting in July, 2001. Both deal with protecting specific personal information, both have an opt-in/opt-out regimen, both limit disclosure of protected information, both require privacy notices, disclosures, and written authorization in certain circumstances.

Here is a summary of the HIPAA privacy rule.

Who. The HIPAA rule applies to "covered entities," which are defined as "health plans, health care providers, and health care clearinghouses." Reflecting on the discussion above about the lack of clear guidance on many HIPAA provisions, not all authorities agree on whether or not this includes insurance agents. Some have even suggested that when carrying out certain functions, insurance agents are not "covered entities," but while performing other functions, they are, or might be, "covered entities."

This is a critical distinction, because “covered entities” are required to fulfill all the core obligations of HIPAA (discussed below).

Health insurers are clearly “covered entities.”

Another key entity under HIPAA is a “business associate,” which nearly all authorities agree could include an insurance agent. In general, “business associates” perform certain functions for “covered entities,” and include a wide range of professions and occupations.

“Covered entities” may share protected health information with “business associates” only if there is a “business associate agreement” in place between them. While the HIPAA rules do not specifically apply to “business associates,” through the “business associate agreement” they have with “covered entities,” “business associates” agree to have certain safeguards and procedures in place to conform to the privacy requirements of HIPAA.

What. The privacy rule applies to “protected health information (PHI),” which is defined as “individually identifiable health information.”

How. Compliance with the privacy rule has four general requirements for “covered entities.”

1. Privacy Notice. Similar to GLBA, a “covered entity” must provide a Privacy Notice to recipients of health care and health insurance benefits.

2. Limited disclosure of PHI. “Covered entities” may disclose PHI without the written authorization of the individual only under very limited circumstances, such as “treatment, payment, and health care operations,” and several other specified situations.

Any other disclosures require the written authorization of the individual, which is considered an “opt-in” approach. Early indications are that many “covered entities” are obtaining written authorizations at initial contact with individuals, as an expedient way to guarantee compliance.

3. Access to records, and accounting of disclosures. Similar to the FCRA, individuals have a right to access their PHI in the custody of “covered entities,” and to request amendments or corrections as appropriate. In addition, “covered entities” must disclose upon request of the individual, an “accounting of disclosures” of PHI made by the “covered entity” or its “business associate” for the previous six years.

4. Administrative requirements. “Covered entities” must implement a number of organizational and procedural guidelines to ensure compliance with all HIPAA requirements.

Excepted benefits. The scope of HIPAA privacy rules involves only a very small portion of insurance coverage lines. Those not under HIPAA are called "excepted benefits," and include life insurance, casualty, accident, disability, liability, workers' compensation, automobile medical payments, credit-only, and a few other incidental types.

Minimum necessary. Another way HIPAA attempts to protect PHI is through the "minimum necessary" rule. According to HHS, it requires that a "covered entity" use, disclose and request only the "minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request."

According to some experts, it is anticipated that this could restrict needed information in a number of ways, such as claims management by third parties. In addition, certain types of loss runs might be impacted, as has been the case in some instances under GLBA.

De-identified information. Another approach that HIPAA takes in protecting PHI is to allow unrestricted use of information that has been sanitized or "de-identified" of any information that would reveal PHI about individuals. What would be left is generic information on treatment, care, claims, and so forth, but nothing that would identify a particular individual.

As with the "minimum necessary" rule, some insurance experts are concerned that insufficient information will be available through the "de-identification" process to allow for some normal and necessary insurance functions.

Authorizations must be specific. As discussed above, no disclosure of PHI is permitted without a written authorization of the individual, except for "treatment, payment, or health care operations," (and a few additional specific circumstances).

In addition, one of the "excepted benefits" under HIPAA is life insurance.

However, in the HHS/OCR "Summary of the HIPAA Privacy Rule," is the following statement. *"An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes."* [Emphasis added.]

As a result, a number of life agents report being required by insurers to get written authorizations signed by prospects/applicants.

Penalties. There are both civil as well as criminal penalties possible for violations of the HIPAA rules. The HHS may impose civil money penalties on a "covered entity" of $100 per failure to comply with the privacy rules, up to a maximum of $25,000 per year.

Criminal violations are handled by the Justice Department. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one year in prison. For violations involving false pretense, the penalties are $100,000 and up to five years in prison. If the violation includes the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, the penalties are $250,000 and up to ten years in prison.

Privacy recommendation for all agencies. Whether agencies are "covered entities" or "business associates" is certainly important. But this should not distract agency managers from the larger issue of insuring strict compliance with all privacy laws, whether HIPAA, GLBA, or FCRA.

One important recommendation made by E&O attorneys is that each agency develop a privacy policy for their employee handbook, and train all employees on the key requirements of the various federal privacy laws.

Resources. Given the broad spectrum of businesses, organizations and professions impacted by HIPAA, there is a considerable amount of information on HIPAA available on the Internet. For example, a recent search on Google turned up 708,000 hits.

However, much of the information is geared to health care professionals. There is actually not a great deal of information for independent agents to turn to.

Here are a few of the resources that might be helpful.

1. The **HHS/OCR** has excellent information on their website: http://www.hhs.gov/ocr/hipaa/

There are several useful documents here, both on this web page, as well as by connecting to links from that page.

Look for "Summary of the HIPAA Privacy Rule," which is a 23-page PDF document.

At http://www.hhs.gov/ocr/hipaa/finalreg.html is a document on the "Final Modifications to the Privacy Rule" (93 pages in PDF format). Also on this page is the "October 10, 2002 Complete Privacy Rule Text, as modified," which is 42 pages.

At http://www.hhs.gov/ocr/hipaa/whatsnew.html scroll down to the entry for 12/04/02, and click on "OCR Guidance Explaining Significant Aspects of the Privacy Rule," which is a 123-page document with an FAQ section at the end of each chapter.

2. **The Independent Insurance Agents and Brokers of America (IIABA)** has an excellent report on HIPAA. To get the full report visit the IIABL website at www.iial.com and click on Technical Issues.

NECESSARY ACTION: Circulate this Technical Advisory to all agency staff.