Click here to return to the Table of Contents

PRIVACY ISSUES IN ADJUSTING CLAIMS IN VIRGINIA AND WEST VIRGINIA: HIPAA AND THE GLBA AND THE GAPS IN BETWEEN

David M. Kersey, Esquire
Hud McClanahan, Esquire
Brewster, Morhous, Cameron, Caruth, Moore, Kersey & Stafford, PLLC
418 Bland Street, Post Office 529
Bluefield, West Virginia 24701
(304) 325-9177

February 5, 2004

Introduction

If you ask the average person on the street about privacy, you will probably get a response similar to this: "I have a constitutional right to privacy." Interestingly, the word "privacy" is not mentioned in the United States Constitution. The United States Supreme Court and Congress have undoubtedly created many "rights to privacy," and privacy appears to be one of the hottest topics of the early Twenty First Century. The existence of a "right to privacy" in medical records evolved from the United States Supreme Court decision in *Whalen v. Roe,* 429 U.S. 589 (1977), in which the Court found that the facts did not rise to the level of a constitutional violation. [1]

Presently politicians and the public face a political phenomenon known as "the privacy issue." Insurers, financial service providers, and health providers whose operations require the efficient use of personal information stand in its path.

While many lawyers and academics can make a career covering privacy issues in various industries, this presentation is limited to privacy rules as they relate to adjusting claims in Virginia and West Virginia. This paper will give a brief overview of the major federal statutes influencing these rules and will try to provide a basic framework for how Virginia and West Virginia have attempted to comply with the federal statutes, and what effect these statutes and regulations have on the claims process.

---

[1] Raymund C. King, *Invasion of Privacy: A New Frontier for Mass Tort Litigation Thanks to HIPAA,* 6 Tort Source (newsletter of the ABA Tort Trial and Insurance Practice Section) 1 (Fall 2003).

I. The *Gramm-Leach-Bliley Act (GLBA) Title V Privacy Rule* and the Dept. of Health & Human Services Privacy Standard under the *Health Insurance Portability and Accountability Act (HIPAA)* create potentially different rules for each state. [2]

The *Gramm-Leach-Bliley Act (GLBA) Privacy Rule* and the Privacy Standard under the *Health Insurance Portability and Accountability Act (HIPAA)* are each infused with the "federal floor" doctrine, establishing a "reverse preemption" phenomenon that any more restrictive state measure must apply and thus be part of an entity's privacy policy. Under both laws, any more restrictive state laws must be woven into the federal compliance in that state. To comply with federal law, therefore, one must identify these state directives, compare them with the federal requirements, then carefully fold them into the privacy program and notice procedures applicable in each state. Accordingly, HIPAA and GLBA are only abstractions. For purposes of compliance, the applicable federal privacy laws are GLBA and HIPAA but only *as modified* by each state's applicable privacy law, and each state is unique.

The process of configuring a given state's application of HIPAA and GLBA is daunting. In the first place, it is not easy to find the "law" in every state. State privacy directives are scattered everywhere and vary by subject matter. In some cases they are buried deep in case law. Often, they are *not* based upon the fundamental privacy principles of Notice, Choice, Access and Security underlying GLBA and HIPAA. Some are conceptually tied to individual "property" rights. Others turn on the meaning of "privilege" or "confidentiality," or words like: "secure" and "private." These

[2] Material used in this section adapted from Chris Gallagher, *The Perfect Storm: GLBA-HIPAA Convergence Episode II*, <http://www.gclaw.com/resources/financial/storm.html> (June 28, 2002).

fundamental disparities with federal privacy directives thus require comparisons of "apples to oranges."

In addition, GLBA and HIPAA do not have matching "federal floors." HIPAA is totally preemptive, *except* for any "provision of state law [that] relates to the privacy of health information *and* is more stringent." 45 C.F.R. § 160.203(b) (2001). "More stringent" is carefully defined at 45 C.F.R. § 160.202 (2001), but again, the process of actual comparison is necessarily subjective. GLBA's federal "floor," set forth at Sec. 507 (the so-called "Sarbanes Amendment"), is quite different from HIPAA's more traditional preemption approach. It is set forth in full below.

> SEC. 507. RELATION TO STATE LAWS.
>
> (a) IN GENERAL. — This subtitle and the amendments made by this subtitle shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subtitle, and then only to the extent of the inconsistency.
>
> (b) GREATER PROTECTION UNDER STATE LAW. — For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subtitle if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subtitle and the amendments made by this subtitle, as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 505(a) of either the person that initiated the complaint or that is the subject of the compliant, on its own motion or upon the petition of any interested party.

Gramm-Leach-Bliley Act Pub. L. No. 106-102, § 507, 113 Stat. 1338 (1999).

GLBA's "greater protection" standard triggers even more "apple to orange" comparisons and, compared to HIPAA, GLBA offers little guidance. It is already clear,

however, that there are circumstances where a state law would provide "greater protection" under GLBA, but may *not* be "more stringent" under HIPAA. For example, HIPAA's special treatment of certain information involving minors is not matched in GLBA, where the sharing of such information may provide "greater protection." *See* 45 C.F.R. § 160.202 (2001) (defining "*More Stringent*"). To be sure, the courts or the Congress will clarify this some day, but again, compliance is required now. Health insurers, contractually bound to HIPAA through providers, health plans and TPA's with similar ties, are subjected to GLBA enforcement through the NAIC Model Rule, a state law. For them, the comparison process promises to be even more complex. Regulators have promised to be understanding during the transition. Attorneys general and class action litigants may not be as congenial.

State-by-state analysis comparing existing state law with the provisions of GLBA and HIPAA is an arduous process, but not impossible. The greater threat is that states may produce *more* legislation to wade through, because despite the comprehensive sweep of the new federal privacy regulations, pro-privacy activists want even more restrictions, and they view the "federal floor" doctrine as an express invitation to enact them. The balances so carefully achieved in GLBA and HIPAA are already tipped toward being more restrictive by their interaction with more restrictive existing state law. Enacting more restrictive laws, in 50 different states, will further tip the balance towards "restrictive." More laws will also increase today's counterproductive complexity.

II. HIPAA application to the claims process in West Virginia and Virginia.

While health insurers and medical providers face new challenges in handling personally identifiable health information, the property and casualty lobby managed to convince lawmakers to give claims handlers a regulatory break; however, even though the claims process appears to have been excluded from HIPAA by definition, the rules for what an insurer can do with *medical information* upon closing the claim have changed. As this article will discuss later, the first questions claims adjusters and support staff should ask upon receipt of *medical information* are:

(1) Whose *medical information* is this?

(2) From whom did I receive it?

(3) What limitations, if any, do the authorizations, subpoenas, and/or protective orders place on the use of the information?

These questions are extremely important to bridge the void left by HIPAA. For while both HIPAA and the GLBA appear to exclude the claims adjusting process, the documents authorizing the release of medical information will most likely limit how or if the information may be retained for future reference or use.

A property and casualty insurer is expressly exempted from HIPAA because a property and casualty insurer is not a "covered entity" as defined by the regulations. A review of 45 CFR §160-103 reveals that the section defines a "covered entity" as "(1) a health plan, (2) health care clearing house and, (3) a health care provider who transmits any health information in electronic form in connection with the transaction covered by the subchapter." A property and casualty insurer clearly

does not meet the definition of a health care clearing house or a health care provider under the definitions in 45 CFR §160-103; however, the definition of health plans specifically excludes property and casualty insurers: "any policy, plan, or program to the extent that it provides, or pays the cost of, excepted benefits that are listed in §2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1) . . . ." The statute sets forth a laundry list of excepted benefits by defining "excepted benefits" at 42 USCA §300gg-91(c) as "benefits under one or more (or any combination thereof)" of the following:

(1) Benefits not subject to requirements
- (A) Coverage only for accident, or disability income insurance, or any combination thereof.
- (B) Coverage issued as a supplement to liability insurance.
- (C) Liability insurance, including general liability insurance and automobile liability insurance.
- (D) Workers' compensation or similar insurance.
- (E) Automobile medical payment insurance.
- (F) Credit-only insurance.
- (H) Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

Obviously, HIPAA has changed the rules for "covered entities" regarding the release of medical information, while apparently excluding claims adjusting. Unfortunately, the limitations on the retention and future use of the information have increased. HIPAA does not provide clear guidance to claims adjusters in either the statutes or the regulations; instead, claims adjusters must *read* the medical authorizations, subpoenas and/or protective orders that enabled them to obtain the information for guidance on how, or if, the medical information may retained for future use.

III. The *Gramm-Leach-Bliley Act (GLBA)* regulations adopted by Virginia and West Virginia.

In order to simplify the potential confusion, members of the National Association of Insurance Commissioners (NAIC) adopted model regulations based upon the GLBA regulations promulgated by several federal agencies. The basis for the adoption of the NAIC model was to provide state insurance departments with a model to implement the Title V privacy provisions of the GLBA.

Based upon the GLBA and the NAIC's model regulations, insurers must meet basic privacy requirements. While the privacy provisions of Title V are quite complex, the main focus of the Act is that financial institutions, including insurers, can share virtually any non-public personal information with affiliated companies, and can only share non public personal information with nonaffiliated companies if the notice provisions of the Act are strictly followed. The following are the basic privacy requirements of GLBA:

1. Privacy Policy -- Each insurer must implement a privacy policy which describes its practices of collecting non-public personal financial information. In addition, the privacy policy must disclose the extent to which it discloses that information for any purpose other than its normal business operations.

2. Privacy Notice -- Each insurer must provide a privacy notice detailing its privacy policy and practices, to its customers and to consumers under certain circumstances. The GLBA distinguishes between customers and consumers. A consumer under the Act would be those who have not yet established a customer relationship such as an applicant. A privacy notice must also be sent applicants, and to non-customer claimants when non-public personal financial information will be used for marketing purposes with a nonaffiliated party. A privacy notice must be sent to customers when the relationship is established and annually

thereafter.

3. Opt Out -- Each insurer must provide every customer and claimant with the opportunity to opt out from having their non-public personal financial information shared for marketing purposes with a nonaffiliated third party. The only exceptions are for information shared with a service provider or with a financial institution in a joint marketing agreement.

4. Opt In -- An insurer may not disclose anyone's non-public personal medical information for marketing purposes, unless that person has given specific affirmative written or electronic approval. These requirements apply equally to consumers and customers. This opt in authorization expires automatically after two years, unless an earlier expiration date is stated.

5. Business Use of Non Public Personal Information -- An insurer may share non-public personal financial and medical information for non-marketing business operations without consent.

A. West Virginia

West Virginia adopted "physical" privacy regulations at C.S.R. 114-62-1 *et seq.* and "handling" privacy regulations at C.S.R. 114-57-1. The "physical" privacy rules deal with the types of equipment and security features insurers must have to protect information.[3] The "handling" rules set forth the rules for disclosing nonpublic personal financial and health information.

---

[3] The "handling" rules constitute the real implementation of GBLA and have already sparked litigation related to the claims handling process. In September 2003, the West Virginia Supreme Court of Appeals heard oral argument in *Nationwide Mutual Insurance Company v. Martino,* Case No. 31270. The case concerns (3) certified questions from the Circuit Court of Harrison County:

1. Does the West Virginia Privacy Rule and the GLBA restrict the dissemination by an insurance company of "nonpublic personal information" regarding an insured or any other person to a claimant or a claimant's legal representative necessary for the proper adjustment of a claim.

West Virginia adopted privacy rules through West Virginia Code § 33-6F-1, which provides in full:

> (a) No person shall disclose any nonpublic personal information contrary to the provisions of Title V of the Gramm-Leach-Bliley Act, Pub. L. 106-102 (1999).
>
> (b) On or before the first day of July, two thousand one, the commissioner shall propose rules for legislative approval in accordance with article twenty, chapter twenty-nine-a of this code necessary to carry out the provisions of Title V of the Gramm-Leach-Bliley Act, Pub. L. 106-102 (1999) and this article.

"Nonpublic personal information" is defined at W.Va. C.S.R. 114-57-2.19 and means "nonpublic personal financial information" and "nonpublic personal health information." Interestingly, the salient regulations do not deal simply with nonpublic personal information, but keep the rules regarding the disclosure of nonpublic personal financial information and nonpublic personal health information separate.

West Virginia regulations require a licensee (insurer) to provide "clear and conspicuous notice" to a consumer before disclosing nonpublic financial information about the consumer to a nonaffiliated third party unless the disclosure falls under certain exceptions. W.Va. C.S.R. 114-57-3.1. While the exceptions are numerous,

---

2. Does the West Virginia Privacy Act and the GLBA restrict the dissemination by an insurance company of "nonpublic personal information" regarding an insured or any other person through the civil discovery process to a claimant/plaintiff once civil litigation is instituted against an insured?

3. To what degree do the West Virginia Privacy Rule and the GLBA provisions restricting dissemination by an insurance company of "nonpublic personal information" regarding an insured or any other person control an insurance company's duties under the West Virginia Trade Practices Act, W.Va. Code § 33-11-1.

The case centers on whether Nationwide acted properly in refusing to provide plaintiff's counsel the name and address of Nationwide's insured so the plaintiff could serve process upon Nationwide's

for the purposes of claims adjustments, a licensee is not required to give notice to the consumer to process an insurance product or service the consumer has "request[ed] or authoriz[ed]." W.Va. C.S.R. § 114-57-13.1(a). This also includes claim processing and underwriting. W.Va. C.S.R. § 114-57-13.1(b)(1) and W.Va. C.S.R. § 114-57-13.1(b)(5). A licensee is also not required to give the consumer notice of the disclosure when the disclosure takes place to "protect against actual or potential fraud or unauthorized transactions. W.Va. C.S.R. § 114-57-14.1(c).

West Virginia's GLBA regulations also cover "nonpublic personal health information." The regulations define "nonpublic personal health information" as "health information that identifies an individual who is the subject of the information; or with respect to which there is a reasonable basis to believe that the information could be used to identify an individual." W.Va. C.S.R. § 114-57-2.21. The regulation regarding "nonpublic personal health information" initially strictly prohibits the disclosure of nonpublic personal health information: "A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed." W.Va. C.S.R. § 114-57-15.1. These authorizations cannot be valid for more than twenty-four months. W.Va. C.S.R. § 114-57-16.1(e). But while the regulations initially prohibit disclosure, W.Va. C.S.R. § 114-57-15.2 provides a very broad exception for the use and disclosure of nonpublic personal health information in the claims process:

---

insured. Nationwide claims that the privacy rule provisions of C.S.R 114-57-1 *et seq.* prohibit it from

> Nothing in this section *shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance*; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; *any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services*; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

(emphasis added).

While the GLBA regulations appear to exempt property and casualty claims procedures outright, the question still remains as to whether property and casualty insurers must comply with HIPAA authorizations when receiving information. This matter will be discussed following the discussion of the Virginia privacy statute.

---

disclosing the information to a nonaffiliated third party.

In 2002, the West Virginia Legislature amended the Unfair Trade Practices Act of West Virginia Code § 33-11-4 to include a new subsection, which that provides that a violation of the West Virginia privacy rules constitutes and unfair trade practice:

> (12) *Failure to maintain privacy of consumer financial and health information.*- Any licensee who violates any provision of the commissioner's rule relating to the privacy of consumer financial and health information shall be deemed to have violated the provisions of this article: Provided, That any licensee who complies with the provisions of this subsection, a commissioner's rule, or a court order shall not be deemed to be in violation of any other provisions of sections three and four of this article by their compliance with this subsection, the rule or court order. For purposes of this subsection, "licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to this chapter.

Interestingly, the provision appears to provide absolute immunity if the licensee complies. Therefore, strict adherence to the "enabling documents" is required to avoid running afoul of the West Virginia Unfair Trade Practices Act.

B. Virginia

Virginia has the distinction of being the first state to integrate the 1982 Model NAIC privacy rules with the new requirements of the GLBA. Virginia combined the two sets of rules by statute rather than regulation. *See* Code of Virginia §§ 38.2-600 through 38.2-619.[4]

The Virginia statute applies to property and casualty insurers who "[c]ollect, receive or maintain information in connection with insurance transactions

involving policies, contracts or certificates of insurance . . . ." Va. Code Ann. § 38.2-601(A)(2). The rights of the Virginia statute are granted to "natural persons" who "are the subject of the information collected, received or maintained." Va. Code Ann. § 38.2-601(B)(2)(a).

Virginia defines "privileged information" to include both financial and health information:

> 'Privileged information' means any individually identifiable information that (i) relates to a claim for insurance benefits or a civil or criminal proceeding involving and individual, and (ii) is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual.

Va. Code Ann. § 38.2-602.

Like West Virginia, Virginia sets time limits on the validity of authorizations for personal or privileged information. In the context of obtaining information in connection with a claim for benefits under an insurance policy, the authorization is valid for "the term of coverage of the policy if the claim is for an accident and sickness insurance benefit; or the duration of the claim if the claim is not for an accident and sickness insurance benefit." Va. Code Ann. § 38.2-606(7)(b).

While Va. Code Ann. § 38.2-608 requires insurance companies to provide individuals who request their personal information with information the insurance company has about the individual, the insurance company does not have to provide information about the individual "that relates to and is collected in connection with or

---

[4] For a thorough review of state by state privacy rules, see J. Stephen Zielezienski & Catherine I. Paolino, *Insurance Privacy After Gramm-Leach-Bliley – Old Concerns, New Protections, Future Challenges,* 8 Conn. Ins. L.J. 315 (2001-2002).

in reasonable anticipation of a claim or civil or criminal proceeding involving them." Va. Code Ann. § 38.2-608(F). This provision appears to allow for the indexing of past claims for future use, unless the information is restricted by the authorization, subpoena and/or protective order.

As for the actual disclosure and use of the personal information, insurance companies are generally prohibited from doing so without an authorization from the individual. Va. Code Ann. § 38.2-613(A). An insurance company may, however, disclose privileged information (financial and medical) without written authorization if the disclosure is to a person other an insurance institution, agent, or insurance-support organization provided the disclosure is "reasonably necessary to detect or prevent criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with insurance transactions." Va. Code Ann. § 38.2-613(B)(2).

The most important part of Virginia's statutory scheme in the eyes of individual adjusters and staff members is the immunity provision. Section 38.2-618 provides absolute immunity for *persons,* not corporations, for certain enumerated disclosures:

> No cause of action in the nature of defamation, invasion of privacy, or negligence shall arise against any person for disclosing personal or privileged information in accordance with this chapter, nor shall such a cause of action arise against any person for furnishing personal or privileged information to an insurance institution, agent, or insurance-support organization. However, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

Evidently the Virginia General Assembly realized the complexity of the privacy statutes and the potential for inadvertent disclosures. The question is whether West Virginia will provide the individuals working in the West Virginia insurance industry the same protection or whether any future causes of action will involve individual claims adjusters and/or administrative assistants.

IV. CONCLUSION: The not-so-noticeable gap between HIPAA and GBLA when records are used beyond the scope of the authorization or protective order.

The most important rule of the new world of privacy for claims adjusters may be stated simply: *Read the medical authorizations, subpoenas, and/or protective orders that enabled the information to get to you.* This rule requires each person who handles personal information, especially medical, to ask the three (3) questions mentioned in section II of this paper: Whose *medical information* is this? From whom did I receive it? What limitations, if any, do the authorizations, subpoenas, and/or protective orders place on the use of the information?

As the above discussion sets forth, insurance companies are generally afforded great latitude in disclosing personal information (financial and medical) in the claims process. Exempted from HIPAA and excepted for the most part from the GLBA, it would appear that insurance claims adjusters can apparently go about business as usual in adjusting, indexing, and referring to old claims. Unfortunately, there may be one area that the regulation and statute writers have yet to address that may be fertile ground for plaintiffs' lawyers: What happens when the retention of the medical

information obtained exceeds the scope of the medical authorization or protective order under which is was obtained?

For example, a reputable insurance company's current "HIPAA compliant" medical authorization states that it will be used for the "purposes of handling [claimant's] Medical Payment and Medical Payment claim(s)." The form goes on to provide a very broad "Use of Information" disclaimer that basically says the company will index and retain the information for other purposes. Arguably, the form is not HIPAA compliant because the scope of the use has been expanded beyond the medical payments and potentially becomes part of the insurance company's index. In order to avoid running afoul of HIPAA, the form should probably state that the information will be used to handle any medical claim which the individual may have that may involve the insurance company on the particular date of loss.

A different, and perhaps more difficult to remedy problem occurs in the context of a subpoena or protective order. For example, an insurance company's lawyer obtains personal nonpublic medical information through a protective order or subpoena that provides that the medical information and copies will be returned or destroyed at the conclusion of the action. The information is copied and passed to the insurance company's adjuster. The adjuster indexes and files the information for future use. If the individual later learns that the medical information has been retained or used in another proceeding, the individual will likely have an action for breach of contract, invasion of privacy, or another cause of action *de jour* for not following the HIPAA requirements in the documents.

The simplest solution for insurance companies is to determine how it received the medical information. This means that the "enabling document," i.e., the document that allow for the release of the records must be carefully scrutinized. In short, insurance companies should not be lulled into complacency just because HIPAA and the GLBA provide latitude in adjusting claims.