The Insurance Federation of Pennsylvania, Inc.

1600 Market Street
Suite 1520
Philadelphia, PA 19103
Tel: (215) 665-0500 Fax: (215) 665-0540
E-mail: mailbox@ifpenn.org

Samuel R. Marshall
President & CEO

September 19, 2002

Original: 2257

Robert C. Nyce
Executive Director
Independent Regulatory Review Commission
14th Floor
333 Market Street
Harrisburg, Pennsylvania 17101

Re: Regulation 11-209 - Insurance Department's Privacy of Consumer Health Information Regulation

Dear Mr. Nyce:

The Insurance Federation supports the Insurance Department's health privacy regulation and recommends the Independent Regulatory Review Commission approve it at your September 26 public meeting. Our support, however, is subject to two clarifications.

First, throughout the promulgation process, we have asked the Department to state explicitly that nothing in the regulation is intended to alter the the flow of health information under the current operations of the Department of Labor and Industry's Workers Compensation Bureau and its administrative processes. Our understanding from communications with the Department is that the Bureau's operations fall squarely within the insurance function exceptions found at Section 146b.11(b)1-33, and that the sharing of personal, non-public health information of workers compensation claimants for purposes of processing and resolving claims therefore will not be subject to the customer authorization requirements of the regulation.

We recommend that the Commission call on the Insurance Department to confirm this representation for the public record on the 26th orally or in writing.

Second, the Department has added a sentence to Section 146b.11(D) stating that it may hold licensees liable for actions of third parties in violation of the regulation. While the regulation's preamble sets out generally the standard the Department will use to assess liability to licensees for third party actions, we seek a clearer understanding of how the Department will use its prosecutorial discretion in such cases.

We understand that the Department will soon promulgate a new Chapter 146c, "Standards for the Safeguarding of Customer Information." We have asked the Department to include in it explicit licensee standards for safeguarding personal, non-public health information that is shared with third parties so that our members can understand the Department's expectations with regard to Section 146b.11(D). We would appreciate it if the Department would confirm this intention on the record on the 26th.

Thank you for the opportunity to comment on this regulation.

Sincerely,

Samuel R. Marshall

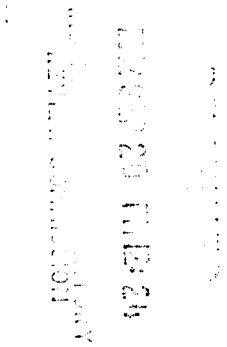
c: Honorable M. Diane Koken
Peter Salvatore
Fiona Wilmarth

IRRC

From: IFP [mailbox@ifpenn.org] Original: 2257
Sent: Friday, September 20, 2002 12:50 PM
To: mailbox
Subject: Regulation 11-209 - Insurance Department's Privacy of Consumer Health Information Regulation

Attached please find a letter from Sam Marshall.

Thank you.



Salvatore, Peter

From: Kockler, Kimberly [Kimberly.Kockler@bcnepa.com]
Sent: Friday, April 12, 2002 4:28 PM
To: 'Salvatore, Peter'
Cc: Davis, F.Kelly; Savitsky, Trish
Subject: Privacy of Consumer Health Information Regulation

Original: 2257

Mr. Salvatore:

The following comment and recommendation are respectfully submitted on behalf of Blue Cross of Northeastern Pennsylvania (BCNEPA) in regard to the Insurance Department's proposed Privacy of Consumer Health Information regulation published in the March 16, 2002 Pennsylvania Bulletin.

Section 146b.12. - Authorizations - We recognize that the 24-month time limit on consumer authorizations was taken from the National Association of Insurance Commissioners (NAIC) health privacy model. BCNEPA also recognizes, however, that this provision is inconsistent with Health Insurance Portability and Accountability Act (HIPAA) standards that contain no similar limitation. HIPAA standards indicate that an expiration date must be included, but do not prescribe a specific timeframe for expiration. We respectfully request that the Department's health privacy regulation mirror HIPAA in regard to the duration of consumer authorizations for ease of administration in regard to state and federal requirements.

Thank you for the opportunity to comment.

Kimberly K. Kockler
Director, Policy Management
Blue Cross of Northeastern Pennsylvania
717-671-8204
717-671-4115 (fax)
Kimberly.Kockler@bcnepa.com

Original: 2257

April 4, 2002

Peter J. Salvatore
Regulatory Coordinator
Commonwealth of Pennsylvania
Department of Insurance
1326 Strawberry Square
Harrisburg, PA 17120

RE: Privacy of Consumer Health Information, 31 Pa. Code, Ch. 146b

Dear Mr. Salvatore:

I am President of the Pennsylvania Association of Mutual Insurance Companies (PAMIC). PAMIC's membership includes 84 mutual property/casualty companies. The purpose of this letter is to offer comments and suggestions for improvement to the Insurance Department" proposed regulation on consumer health information privacy as published in the March 16, 2002, Pennsylvania Bulletin. I thank you in advance for the attention you and the Insurance Department always afford to our membership's concerns.

The proposed regulation is a stand-alone version of Title V of the NAIC Model Privacy Regulation. Title V deals with privacy requirements for personal health information. The Department has done a careful job in modifying and deleting definitions relating to "consumer" and "customer" as found in the NAIC version but not pertinent to the Pennsylvania stand-alone version. The NAIC version also contained definitional overlaps of "financial" and "health" information that would have made certain information subject to both a consumer opt-out right for "financial" and an opt-in for "health' information. The Pennsylvania version has avoided this by inserting (ii) in the definition of "nonpublic personal health information" in Section 146b.2.

The proposed regulation requires that a company that wishes to use the "insurance function exception" (Section 146b.11(b)) to the basic consumer opt-in requirement must enter into an agreement with any third party to which it may disclose information requiring that third party to also use the information solely for the functions stated in the exception. This is not required if the third party is itself an entity licensed by the Insurance Department. I understand what the Department is apparently doing here. It is trying to assure privacy compliance without any gaps when protected information is given to an unregulated entity. However, the proposed regulation also provides that entities in compliance with the Federal HIPAA regulation do not need to comply with this proposed regulation. Section 146b.21.(a). This constitutes a recognition of the comparability of the HIPAA regulation to the proposed regulation and a recognition of the adequacy of Federal government enforcement. It explicitly states that a licensee in

compliance with the Federal regulation "will not be subject to this chapter." Therefore the exception to the third party agreement requirement should be enlarged to include third parties subject to the HIPAA regulation. Surely for a HIPAA regulated third party there is no gap in privacy protection needing to be closed by this kind of agreement. Without this modification, HIPAA regulated entities with which licensees deal could possibly be subjected to conflicting requirements, one Federally mandated, one imposed by contract.

The proposed regulation also contains a major and highly damaging departure from the NAIC Title V. The "insurance function exception" mentioned in the last paragraph is key to the practical workability of the regulation. It exempts licensees from the requirement to obtain affirmative written permission from the consumer (the opt-in feature) before disclosing health information. The exemption applies to disclosures in the course of 33 stated activities that are normal and expected uses of the information for insurance purposes. The NAIC version of its Title V introduced these enumerated exceptions with the recital that:

> "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...." (NAIC Model, Sec. 17(B)

The proposed regulation has substituted in the place of the words I have underlined the following: "to the extent that the disclosure is necessary for the performance of one or more of the following insurance functions..." (Section 146b.11.(b)) This introduces a serious element of uncertainty that will likely cause many companies to simply not use the exception since violation will be a breach of the Unfair Insurance Practices Act. For the exception to be useable it must be clear. Determination of necessity will require each licensee to weigh up each piece of medical information in a document and make a determination of its relevancy to the particular purpose for which it will be used. Careful redaction of otherwise relevant documents will be necessary in every case. Obviously the Department considers there to be a difference between health information that is useful for claims adjustment and health information that is necessary for claims adjustment. If not, the change in language would not have been made. The new standard is narrower, higher, and at the same time more vague. It is for that reason not workable.

It is possible that the drafter has looked to the Federal regulation for guidance in improving the NAIC language. I do not have a copy of the latest draft of the HIPAA regulation, but an earlier summary that I do have shows that entities must make all reasonable efforts not to use or disclose more that the minimum amount of protected health information necessary to provide treatment. This seems to focus the regulation on the screening activity of the entity rather than whether a particular piece of data is or is not "necessary." Setting up such procedures makes sense in the context of health care providers and others subject to HIPAA. Medical care and the financing of such care are the primary purpose of such providers. That is not the case with property/casualty insurers. To take the typical example of a bodily injury auto claim, the health information used would probably be both broader and narrower than that used by an entity subject to HIPAA. Broader, because the information needed to determine

preexisting conditions, fitness for driving, extent of impairment, causation of the accident, would necessarily involve a far broader segment of medical information than would be needed for a simple referral for an in-office medical procedure. Narrower, because property/casualty companies are not normally the repositories of comprehensive medical records of individuals. Medical information comes to them on a claim specific basis by the nature of the claims they handle. While it is true that there may well be insurance entities that are more comprehensively involved with a person's complete medical history, these entities are precisely the ones that will be HIPAA regulated anyway. PAMIC members need a reliable "bright line" definition for the insurance function to be practical.

On March 21, 2002, the Bush Administration proposed some significant changes to the Federal HIPAA regulation. I am sure the Department will want to review these changes to see if any of the departures from the NAIC model are still in the Federal version. It would serve little purpose for property/casualty companies to be more burdened than health care providers in assuring privacy.

Thank you for giving PAMIC opportunities to share member concerns all through this process. As always, I will be happy to answer any questions or comments raised by this letter.

Sincerely,

Steven C. Elliott, J. D., CPCU, CLU
President

CC: P.Raub, PAMIC Chairman
J. Bookhamer, PAMIC GA Chair

The Insurance Federation of Pennsylvania, Inc.

1600 Market Street
Suite 1520
Philadelphia, PA 19103
Tel: (215) 665-0500 Fax: (215) 665-0540
E-mail: mailbox@ifpenn.org

Samuel R. Marshall
President & CEO

April 14, 2002

Original: 2257

Peter J. Salvatore
Regulatory Coordinator
Pennsylvania Insurance Department
Strawberry Square
Harrisburg, PA 17120

Re: Proposed Chapter 146b - Privacy of consumer health information

Dear Mr. Salvatore:

The Insurance Federation, on behalf of our member companies and in conjunction with our national counterparts, offers the following comments with respect to the Department's proposed regulation setting forth its privacy standards for insurers in possession of consumer health information.

At the outset, we note that insurers already have a strong record of protecting the privacy of consumers' health information, and the protections our industry already provides are consistent with those in this regulation. In that sense, we do not read this regulation as intended to bring an end to perceived or alleged insurer abuses of consumers' health privacy, but rather to codify protections already in place consistent with federal and national safeguards.

Our comments reflect this. They are, for the most part, requests for clarification and reasonableness in terms of compliance, as opposed to substantive objections to the underlying protections in the regulation.

That should not diminish the importance of the comments or the need to address our concerns. But we hope these comments are reviewed with the recognition that insurers

are just as committed to privacy as is the Department, with our concern being that the details in the regulation be clear and reasonable.

The importance of privacy should not diminish the importance of achieving it through a clear and reasonable regulation, and it should not be at the expense of accurate and efficient underwriting and claims administration - both of which are as important to consumers as is privacy. We therefore need to address, as much as possible, ambiguities in the regulation - not just to avoid future problems with the Department regarding compliance, but also to avoid disputes among insurers and between insurers and others on the precise requirements of the regulation.

Turning to the specifics of the regulation:

Section 146b.1 - Purpose

Section (a)(3): This subsection refers to consumer "consent," whereas the relevant sections in the regulation refer to "authorization." It also does not refer to the exceptions provided in the regulation.

Accordingly, we recommend this subsection be revised to read that this chapter "requires licensees to obtain the authorization of consumers prior to disclosing nonpublic personal health information, unless otherwise permitted herein."

Section 146b.2 - Definitions

"Consumer:" The inclusion of workers' compensation claimants raises several concerns. First is the concern raised by several national trade associations that workers compensation is not a form of insurance that is used for personal, family or household purposes and is therefore outside the Department's statutory authority.

Beyond this statutory authority concern, we have some concerns of practical implementation if workers compensation claimants

are to be included. We (and, I suspect, the Bureau of Workers Compensation) need clarity from the Insurance Department that nothing in this regulation is meant to alter the nature and means of sharing and disclosure of health information that presently occurs under the workers compensation system.

If the Department does envision that this regulation will require changes in this area, it should clarify precisely what that change is. Otherwise, we will be left with the prospect of violating one set of laws to satisfy another.

Our hope, of course, is that the Department does not envision that this regulation will require any changes in the sharing and disclosure of health information under the workers compensation system, and that it will clearly state this. In considering this issue, you should also consider that the workers compensation system is both insured and self-insured, and that claimants covered under self-insurance plans will not be consumers under this regulation. It makes no sense to have two sets of standards for claimants in that system, depending solely on the funding of their coverage.

"Health information:" This definition differs slightly, but perhaps significantly, from the "health information" definition in this regulation's companion subchapter, Chapter 146a covering privacy of consumers' financial information: This definition adds the exception of "nonpublic personal financial information."

We recommend deletion of this additional exception. As we read the definition of "nonpublic personal financial information," it specifically excludes "health information" through the exceptions listed in the definition of "personally identifiable financial information." Confusing as that seems, the net result is that health information is always an exception to financial information, not the other way around, as this definition would suggest.

Frankly, much of this problem could be resolved if the Department better clarifies two matters: First, that the financial privacy regulation does not apply to claims processing and similar insurance functions, but rather is

limited to information that might otherwise be used in marketing; and second, that the claims exemption applies to third party as well as first party claims (the New York Department issued a clarification on this on December 19, 2001).

In any event, if the Department regards the scope of the "health information" definitions in the two regulations as different, it should at least clarify those differences - and it should resolve any ambiguities as to what constitutes health versus financial information.

"Licensee:" We are not sure what other entities the Department envisions beyond insurers as defined in Section 201-A of the Insurance Department Act. For instance, that definition already includes agents and brokers, and HMOs - so there may be no need to also include them here as an addition to insurers. We recommend that this definition be revised consistent with the "insurer" definition in Section 201-A, and that it clarify the entities the Department intends to include beyond those in the Section 201-A definition.

Section 146b.11 - Required authorization and the "insurance function" exceptions

As a general comment, we recommend the Department clarify, either in the regulation itself or the preamble, that the authorization requirement is generally directed to marketing, not to underwriting, claims administration and other insurance functions. We also recommend the Department expressly include third party as well as first party claims within its claims exception - again, something that could be done in the preamble.

The Department may believe the regulation is already "abundantly clear" on this, as it asserted in its preamble to its financial privacy regulation. Unfortunately, not all insurers see this abundance in the text of the regulation or the Department's comment to date, and it has hampered the routine sharing of information in the claims context,

especially with respect to third party claims. As noted above, the New York Department issued this type of clarification on December 19, 2001; that may serve as helpful precedent.

Subsection (b) - Insurance function exception: We recommend the Department delete the phrase "to the extent that the disclosure of nonpublic personal health information is necessary." As the Department acknowledges, this phrase is not in Section 17(B) of the NAIC model on which this regulation is based; my understanding is that it is also not in any other state's regulation.

Our understanding of the insurance function exception, at least at the NAIC level and we hope in this regulation, is that it is intended to reflect and protect normal business operations of insurers.

The Department's "necessary" phrase is a dangerously ambiguous limitation to this, as "necessary" is a term that can vary among regulators and insurers. For instance, insurers might routinely disclose certain health information in underwriting or claims processing. But the Department could envision, with the perspective of hindsight review, some other way of performing those functions without disclosure and decree that the disclosure is therefore not necessary.

We appreciate the Department's contention that its addition of the "necessary" phrase is consistent with HIPAA. That federal standard, however, is itself vague, and it should not be perpetuated or compounded here - especially given that we have no assurance the Department will follow the same interpretations of "necessary" as will federal regulators.

In the alternative, the Department should at least clarify what it means by "necessary." To that end, if the Department is committed to incorporating a federal standard not found in any other state, we recommend it at least adopt the federal definition of "necessary" found in Section 509 of the GLBA. That section defines disclosures as being "necessary" if they are required, or are a "usual, appropriate or acceptable" method of performing the underlying function.

Subsections (b)(1) and (2): We appreciate that this language mirrors that of the NAIC model. We recommend, however, that the Department offer two clarifications in its preamble. First, the Department should clarify that these subsections apply to third party as well as first party claims (we also recommend the Department clarify the same with respect to its financial privacy regulation).

Second, the Department should clarify that this is a comprehensive inclusion of the claims process. For instance, claims investigation, negotiation and settlement are three routine claims functions that arguably might not fall within claims administration, adjustment and management. We appreciate that is not the result intended here; the Department should clarify this in its preamble.

Subsection (b)(23): We recommend the Department clarify that this includes reporting to various index and consumer reporting bureaus; again, this may be best done through the preamble.

Express acknowledgement of continued reporting to the various bureaus may also help resolve insurer anxiety about sharing information, whether financial or health, with respect to third party claims. Insurers routinely report this information on their claims to bureaus that is subsequently used by other insurers on their claims - thus essentially sharing information on third party as well as first party claims. Clarity on reporting to bureaus may therefore help achieve needed clarity within the industry on the sharing of information on third party claims.

Subsection (b)(31): This is another subsection where a seemingly minor variation from the NAIC model may cause unintended consequences. This subsection covers complying with court ordered warrants, subpoenas or summons issued by various officials. The NAIC model refers to complying with legal process, which suggests situations where information might be shared even in the absence of warrants, subpoenas or summons.

We recommend the Department add the NAIC language to the end of this subsection, stating "or otherwise comply with legal process."

Insurers are under increased pressure to be careful in the health and financial information they release, as evidenced by the October 26, 2001 ruling in Ingram v. Mutual of Omaha, F.Supp.2d (W.D.Mo. 2001) that we shared with you in our November 19, 2001 letter. The court in Ingram ruled that an insurer violated its fiduciary duty to its insured by releasing health information in response to a subpoena without objecting or moving to quash. Regulations such as this will not end the threat of such a ruling. But this regulation should not add to that threat - and this deviation from the NAIC model's reference to a "legal process" exception does just that.

Subsection (c) - Insurance functions performed by third parties on behalf of licensees: We recommend deletion, or significant revision, of this section. It requires that an insurer disclosing health information to a non-licensed third party "enter into an agreement" with a third party prohibiting the third party from disclosing the information for purposes beyond the insurance functions listed in section (b).

The section is not needed - probably the reason it was not included in the NAIC model. First, it should not apply to situations where the consumer has given authorization consistent with section (a) and Section 146b.12. This is really a drafting concern: While the heading in subsection (c) is limited to third parties handling areas covered by the insurance functions exceptions to the authorization requirement, the text here does not have that limit.

Second, it is not needed even if limited to the insurance functions exceptions in section (b). The insurer will be responsible to the Department if a third party acting on its behalf discloses information beyond those exceptions. After all, it is the insurer who is the licensed entity, and it is the insurer - not these non-licensed third parties - against whom the Department will proceed should the third parties go beyond the section (b) exceptions.

Requiring insurers to "enter into agreements" with their third party vendors adds only confusion, not security for consumers. The Department does not gain any enforcement power over the third party through this; if a third party violates an "agreement" with an insurer, the Department is still limited to going against the insurer.

Further, we are not sure what the Department means by an "agreement." Is this a contract? If so, this would impose a significant burden on insurers, for no gain in terms of privacy protection. It also raises a number of basic contractual concerns. For instance, what is the consideration; what is the damage to the insurer if the third party violates the contract?

Finally, we question the Department's statutory authority to do this. Insurers routinely use third parties to handle any number of insurance functions, many of which are regulated under Pennsylvania's insurance laws. We know of no other instance where the Department requires insurers to "enter into agreements" binding third parties to compliance with the insurance laws, and we do not believe the Department has the authority to do so here.

If the Department wants insurers to take affirmative steps to ensure that their vendors are aware of and comply with the limits of the insurance functions exceptions in section (b), it could require that insurers send out an annual notice of this to each of their vendors. That is a much simpler way of ensuring the goal of this section - that vendors be aware of the privacy limits in this regulation.

Section 146b.12 - Authorizations

Subsection (b) - Duration of authorization: We recommend the Department consider allowing authorizations to last for 30, not 24, months, at least for life insurers. A number of life insurers raised this problem because their incontestability periods last for 24 months; if something comes up at the end of the incontestability period, the insurer may need up to six months to resolve the problem.

This concern may be alleviated by clarifying that the exceptions authorization requirement are of unlimited duration, which I read as their intent. The difficulty is that life insurers tend to get authorizations even for some of the functions included in the "insurance functions" exceptions. Granted, they could begin limiting their authorizations. But that seems a penalty for providing more privacy than this regulation would require; the better solution is to extend their authorization period for 30 months.

Subsection (d): Record of authorization: We question the need for this subsection and its length. First, my admittedly quick review of the related financial privacy regulation and the "banks selling insurance" provisions in the Insurance Department Act does not uncover a similar record retention period for opt-out notices, essentially the financial equivalent of these authorizations. I am not sure why one is needed here.

Second, six years is too long; by way of example, the Department requires only three years for record retention of life illustrations, and I believe it requires records of complaints for a similar period.

As a practical matter, insurers will keep these records for some time to protect themselves from any consumer complaints. This regulation, however, applies only to dealings between the Department and insurers - and there is no need for the Department to go back six years in its review of insurers and any authorizations they receive.

Section 146b.24 - Compliance dates

The reference to "annual receipts" is confusing. We read this, from an insurer's perspective, to mean annual premiums, meaning that veritably all of our members will be subject to the proposed April 14, 2003 date - but the term "receipt" should be clarified to mean premium.

Further, we are not sure what this means for producers, who are also defined as "licensees" under this regulation. I am not sure a producer ever has "receipts," or even premiums, as he collects them only on behalf of an insurer. This could create an unintended loophole for producers to escape complinace with the

More important, we believe the April, 2003 compliance date is unreasonable unless the Department deletes the "agreement" requirement between insurers and third party vendors in Section 146b.11(c). If we are required to obtain separate agreements with every vendor acting on our behalf who might handle health information, it will take a period of time considerably longer than provided here.

As always, we appreciate the opportunity to comment on this, and we look forward to working with the Department and the IRRC to resolve these concerns and implement this regulation.

Sincerely,

Samuel R. Marshall

Alliance
of American Insurers

REYNOLD E. BECKER
Vice President – Property/Casualty
rbecker@allianceai.org

March 21, 2002

Original #2257

Peter J. Salvatore
Regulatory Coordinator
Insurance Department
1326 Strawberry Square
Harrisburg, PA 17120

Dear Peter:

Privacy of Consumer Health Information
31 PA.CODE CH 146b

The Alliance of American Insurers is a national trade association with 330 property/casualty insurance company members. Alliance member companies write both personal and commercial lines policies in Pennsylvania.

Our member companies wish to comply with the letter and spirit of the *financial* privacy provisions of the Gramm-Leach-Bliley (GLB) Act. We previously commented on Chapter 146a, dealing with financial information, separately. We commend the Department for handling health information privacy on a separate track, and recognizing the significance of the April 13, 2003 effective date for U.S. Department of Health and Human Services (HHS) rules.

This proposed regulation is patterned after the health portion of the 2000 National Association of Insurance Commissioners (NAIC) model privacy regulation. As we noted in our letter of August 27, and orally during the August 28, 2001 outreach meeting, the Alliance and its member companies, as well as much of the property/casualty insurance industry, are opposed to the health portion of the NAIC model as presently written.

Consistency With Statues

Section 504(a)(2) of GLB requires that regulations prescribed by "state insurance authorities" be "consistent and comparable with the regulations prescribed by the other agencies..." Those other agencies are the federal regulators of banking and securities.

This proposed regulation is *not* required by federal law, *not consistent* with GLB, and not *consistent* with federal banking and securities rules:

- The proposed regulation goes far beyond the scope of Title V of GLB, which deals only with *financial* information, *never* mentioning *health* information. The proposal cites no Pennsylvania statute specifically requiring or authorizing regulations on health information privacy.

3025 Highland Parkway, Suite 800 • Downers Grove, Illinois 60515-1289
tel: 630.724.2109 • *fax:* 630.724.2190 • www.allianceai.org

- No health information privacy rules have been adopted by federal banking and securities regulators. The staff commentary to those federal rules gratuitously attempt to treat health information gathered as part of a financial transaction as nonpublic personal information.

- The authorizations mandated by the Department's proposed regulation are *not consistent* with the federal rules. The federal rules adhere to GLB's "opt-out" system, which applies only to disclosures to non-affiliated third parties. The Department's proposed regulation would impose a more burdensome "authorization" or "opt-in" system, applicable to both affiliate and non-affiliate disclosures. Taking this approach will place insurers at a competitive disadvantage compared to banks and securities firms.

The proposed regulation also conflicts with the rules finalized last year by HHS under the Health Insurance Portability and Accountability Act (HIPAA). Compliance with the HHS rules is not required until April 13, 2003. The Department has recognized the effective date issue.

Thus, there is no federal or state statute requiring or authorizing the adoption of this regulation. Twelve *other state insurance departments have elected not to pursue the health portion of the NAIC model: Connecticut, Delaware, District of Columbia, Hawaii, Idaho, Illinois, Indiana, Louisiana, Michigan, Missouri, Nevada & Tennessee.*

Reasonableness

The Department asserts that it wishes to achieve a level of uniformity, yet in almost the next breath proposes two significant deviations from the NAIC model regulation. With the possible exceptions of proposed regulations in California and Texas (which, unlike Pennsylvania, have privacy statutes covering health information), no other state insurance department is pursuing:

- A precondition that disclosures be "necessary for the performance" of the listed insurance function exceptions in Section 146b.11(a). Who decides whether the information is necessary? The NAIC intentionally created a list of "safe harbors" for licensees, and wisely recognized that this was unworkable to inject subjective preconditions.
- A requirement that licensees enter into confidentiality agreements with third parties in Section 146b.11 (b). Section 146b.12(a)(3) already requires that the consumer be informed as to those third parties and how the information will be used.

Imposing these Pennsylvania-only requirements will be burdensome and costly for insurers writing in the Commonwealth. These additional costs will ultimately be borne by insurance consumers.

Further, the entire regulation would place an unreasonable burden upon insurers, that are not faced by banks or securities firms under federal regulations.

Fiscal Impact

The Department asserts that "adoption of this proposed rulemaking should not have a significant cost impact over what is currently being required by the federal HIPAA privacy regulation." However, in its background submission, the Department correctly notes that "automobile insurance carriers will not be subject to those regulations" (i.e. HIPAA rules). Neither will workers compensation carriers. Thus, on the contrary, the proposed regulation's new mandates and restrictions will definitely have a significant cost impact for such carriers.

We respectfully request that this proposed regulation be withdrawn. We welcome the opportunity to work with the Department in a deliberative fashion on any future changes needed to Pennsylvania statutes or regulations to harmonize them with the HHS rules.

Sincerely,

Reynold E. Becker

Reynold E. Becker

Copies to: Neil Malady
Keith Bateman
James White
Steve Elliott – PAMIC
Sam Marshall – IFP

G:\PERSLINE\REB\REB2002\PALTRHEALTHPRIVREG.DOC

American Insurance Association

1130 Connecticut Ave. NW
Suite 1000
Washington, DC 20036
202-828-7100
Fax 202-293-1219
www.aiadc.org

September 12, 2001

BY E-MAIL

Original: 2257

Peter J. Salvatore
Regulatory Coordinator
Insurance Department
Commonwealth of Pennsylvania
1326 Strawberry Square
Harrisburg, PA 17120

RE: AIA Comments on Pennsylvania Draft Regulation (08/14/01): Chapter 146b, "Privacy of Consumer Health Information"

Dear Mr. Salvatore:

The American Insurance Association ("AIA") is a national trade association representing more than 370 property and casualty insurers that write insurance in every jurisdiction in the United States. The U.S. premiums for AIA's member companies exceed $75 billion each year. AIA member companies offer all types of property and casualty insurance, including personal and commercial automobile insurance, commercial property and liability coverage, workers' compensation, homeowners' insurance, medical malpractice coverage, and product liability insurance. AIA represents companies writing both personal and commercial lines of business in the State of Pennsylvania. In 1999, AIA member companies wrote almost $2.8 billion in premiums in Pennsylvania. We are pleased to provide comments on draft regulation Chapter 146b, "Privacy of Consumer Health Information" ("Pennsylvania Health Privacy Regulation" or "Regulation").

AIA supports state efforts to protect consumer information pursuant to Title V of GLBA while preserving critical business use of such information. For AIA member companies, many of which operate regionally and nationally, uniformity and consistency are necessary for three overriding reasons: (1) compliance implementation; (2) reduction in cost burden; and (3) leveling the competitive playing field. The costs of ensuring compliance increase with differing regulation. Those costs will inevitably increase where a company guesses incorrectly about a legislative or regulatory outcome and must re-tool its privacy compliance program. Finally, an uneven insurance regulatory playing field in the area of privacy may tip the competitive balance in favor of federally regulated financial institutions (which are regulated by one standard instead of by 51 standards).

AIA appreciates your consideration of all of the issues raised in these comments. In

particular, we would like to focus your attention on our concerns with the use of the term "necessary" in §146b.11(b) of the Pennsylvania Health Privacy Regulation, as well as the apparent inclusion of a new third-party vendor "agreement" requirement in §146b.11(c). There is the potential for great confusion resulting from the imposition of a standard like this one that differs from the NAIC Privacy of Consumer Financial and Health Information Model Regulation ("NAIC Model Privacy Regulation" or "NAIC Model Regulation").

Privacy of Health Information Regulation Generally

AIA suggests not promulgating the Pennsylvania Health Privacy Regulation at this time.

First, Title V of GLBA was not meant to address nonpublic personal health information. It only explicitly addresses nonpublic personal financial information. (See, 15 U.S.C. §6809(4)(A), "The term 'nonpublic personal information' means personally identifiable **financial** information ..." (emphasis added)). As a result, there is no need to promulgate health information privacy regulations (which were not contemplated by GLBA).

Second, there may be conflicting federal obligations governing the handling of such information, including the federal Health Insurance Portability and Accountability Act ("HIPAA") privacy regulations released by the U.S. Department of Health and Human Services. Since the HHS "health information" regulations have recently been finalized and compliance is not required for some time, it makes sense for the Department to exercise caution in this area of regulation. While the property and casualty insurance sector is not covered by those regulations, the health insurance sector has been engaged in ongoing compliance efforts with respect to the HHS regulations and GLBA. Interposing different health information regulations now would only increase the compliance burden on health insurers and might subject consumers to inconsistent standards when the HHS regulations are finalized.

The remainder of these comments focuses on suggested changes, assuming that the Department intends to make the Pennsylvania Health Privacy Regulation permanent.

Purpose
(See §146b.1(a)(3).)

AIA recommends deleting the provision found in §146b.1(a)(3) relating to preventing disclosure, since it is confusing and misleading.

As drafted, §146b.1(a)(3) reads as follows: "Provides methods for consumers to prevent a licensee from disclosing that information." (Emphasis added). Chapter 146b relates to health information for which a disclosure authorization mechanism is established. "Preventing disclosure" would be applicable in an "opt-out" structure like that described in Chapter 146a relating to financial information – it is out of place in this authorization system. AIA's recommendation to remove this provision will help to avoid unnecessary confusion.

Examples
(See §146b.1(c).)

AIA recommends revising §146b.1(c) relating to examples to more closely follow the NAIC Model Regulation's Rule of Construction.

The Regulation's example provision in §146b.1(c) currently reads: "The examples provided in this chapter are for illustrative purposes only and do not otherwise limit or restrict the scope of this chapter." The Regulation stops short of affording safe harbor protection to those seeking to comply with the Regulation's requirements by following the examples. Section 3 of the NAIC Model Regulation offers rules of construction that lend security to a company electing to use a sample clause with the intent of complying with the regulation. The text of the new section would be as follows: **"The examples in this regulation are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this regulation."**

Definitions
(See §146b.2.)

AIA recommends **adding** several definitions for the reasons provided below:

"**Affiliate**" is used in the AIA recommendation relating to §146b.11(b). (See §4A of the NAIC Model Regulation)

"**Clear and conspicuous**" is used in the delivery of authorization requests requirement, §146b.13 of the Pennsylvania Health Privacy Regulation. (See §4B of the NAIC Model Regulation.)

"**Control**" is used in the definition of "affiliate". (See §4H of the NAIC Model Regulation.)

AIA recommends **revising** the definition of consumer to track the NAIC Model Regulation:

"**Consumer**" – The Regulation includes claimants (including those under a workers' compensation policy) automatically as consumers under the Pennsylvania Health Privacy Regulation. See §§146b.2, "Consumer" (i)(D), (I). This is a departure from their treatment under the NAIC Model Regulation (as well as the Department's financial information privacy regulation). Under the Model Regulation, claimants are only considered to be a licensee's "consumers" where their nonpublic personal financial information is disclosed outside the exceptions identified in Sections 14 through 16. See §§ 4F(2)(d)(i)(II), (ii). Similarly, and perhaps more importantly, workers' compensation claimants under the NAIC Model Regulation are only treated as "consumers" when an insurer (a) fails to give notice to workers' compensation policyholders and (b) discloses nonpublic personal financial information outside the Section 14 through 16 exceptions. See §4F(2)(e). The Regulation's differing definition will only cause confusion among licensees that are used to defining consumer by reference to the NAIC Model Regulation.

Health Information - Marketing Authorization
(See §146b.11(a).)

AIA suggests revising §146b.11(a) to be specifically targeted at marketing (i.e., per the National Conference of Insurance Legislators Privacy Model, the general regulation should be that an authorization is required from customers or consumers before their nonpublic personal health information is disclosed by a licensee for marketing purposes only). Section 146b.11(a) of the regulation would be revised as follows: "A licensee shall not disclose nonpublic personal health information about a consumer or customer **for the marketing of products or services for personal, family, or household purposes** unless an authorization in compliance with Section 3 of this administrative regulation is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed."

The authorization requirement was aimed at marketing disclosures of nonpublic personal health information. To further that intent, §146b.11(a) should identify the specific type of disclosure for which an authorization must be sought.

Health Information – Necessity Standard/Affiliates
(See §146b.11(b).)

AIA recommends deleting language that reads, "to the extent that such disclosure of nonpublic personal health information is necessary" and AIA further suggests adding "or affiliate" in §146b.11(b) after "by or on behalf of the licensee". Section 146b.11(b) would read as follows: "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 **or affiliate**:".

It is unclear why the "necessity" condition is included and whether this condition creates a new standard. Promulgation of a new "necessity" standard would a significant departure from the NAIC Model Regulation. Licensees subject to this standard would have little practical guidance (or experience) determining whether their excepted disclosures of nonpublic personal health information are "necessary" according to the Regulation. We recommend that the Department delete this phrase.

As for the suggested reference to affiliates, since one of the objectives of GLBA is to allow greater flexibility in working with affiliates, adding "or affiliate" brings consistency and clarity to this part of the regulation.

Insurance Functions Performed by Third Parties
(See §146b.11(c).)

AIA recommends deleting §146b.11(c), which imposes new and unmanageable obligations on licensees.

Through the addition of §146b.11(c) – which is not set forth in the NAIC Model Regulation – the Department appears to have added an "agreement" requirement not present in the Model Regulation. This requirement will add enormous cost burdens to routine disclosures of health information to accomplish business purposes, including information management and

recordkeeping costs. Further, to the extent that this new subsection is an attempt by the Department to hold licensees accountable for the actions of third party vendors, AIA strongly objects. Privacy requirements imposed on Pennsylvania licensees should be manageable, not overwhelming. Privacy obligations of the Regulation should depend on a licensee's acts or omissions, not the failure to police others over whom the Department has no jurisdiction.

Violation
(See §146b.23.)

AIA recommends revising the violations section as follows: "Violations of this chapter **may be** ~~are~~ deemed and defined by the Commissioner to be an unfair method of competition and an unfair or deceptive act or practice and **may therefore** ~~shall~~ be subject to applicable penalties or remedies contained in the Unfair Insurance Practices Act (40 P.S. §§1171.1—1171.15)."

The penalties section should not be mandatory, but should give the Commissioner discretion to determine whether penalties are appropriate in a given circumstance. Indeed, the penalties under Chapter 4 of Title 40, which address unfair practices, are discretionary. AIA's proposed revision would allow minor mistakes to be handled in a suitable manner and it would allow penalties to be imposed where the Commissioner deems appropriate.

Effective Date
(See §146b.24.)

AIA suggests revising the effective date provision as follows: "This chapter is effective **60 days from the date of** publication in the *Pennsylvania Bulletin*."

A delayed effective date provides a reasonable amount of time for licensees to prepare for systems and other implementation issues in order to be in compliance with the Regulation.

Ministerial Changes

AIA recommends making the following ministerial changes, as indicated below:

1. Placing the term "Financial institution" in italics (where it is defined in §149b.2).

2. Revising the wording of (i)(B) under the definition of "nonpublic personal health information" found in §146b.2, as follows: "Provides ~~There is~~ a reasonable basis to believe that the information could be used to identify an individual." This change will make the construction of the provision parallel to that found in (i)(A).

3. Revising the wording of §146b.11(b)(31), as follows: "An activity otherwise permitted by law, required pursuant to governmental regulatory or reporting authority, or to comply with legal process (such as a court ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena)." The "legal process" language is consistent with that found in §17B of the NAIC Model Regulation.

4. Revising the manner in which additional insurance function exceptions are published in

§146b.11(d).

Conclusion

In conclusion, on behalf of our member companies, AIA respectfully asks that the above comments be taken into consideration when assessing the Pennsylvania Health Privacy Regulation. We reserve the right to supplement our comments as the process moves forward. Thank you for your attention. If you have questions or comments, please contact Taylor Cosby, Vice President, at 410-267-9581 or Stef Zielezienski, Assistant General Counsel, at 202-828-7175.

Respectfully submitted,

/s/ /s/

Taylor Cosby J. Stephen Zielezienski

MICHAEL J. BARTHOLOMEW
SENIOR COUNSEL, STATE RELATIONS
michaelbartholomew@acli.com

101 CONSTITUTION AVENUE,
N.W., SUITE 700
WASHINGTON, D.C. 20001
TELEPHONE (202) 624-2178 FACSIMILE (202) 572-4708 www.acli.com

AMERICAN COUNCIL OF LIFE INSURERS
FINANCIAL SECURITY

Original: 2257

April 16, 2002

Peter J. Salvatore
Regulatory Coordinator
Pennsylvania Insurance Department
Strawberry Square
Harrisburg, PA 17120

Re: Health Information Privacy Regulation- Proposed Chapter 146b

Dear Mr. Salvatore:

I am writing you on behalf of the 310 life insurers, which are our members, and write 73 percent of the life insurance and annuity business in Pennsylvania.

Those member companies believe and support the principles embodied in the model regulation developed by the NAIC concerning the sharing of non-public personal health information. We are also supportive of the comments made to you April 14, 2002 by Samuel R. Marshall, Insurance Federation of Pennsylvania, to the extent those comments apply to the operations of life insurers.

Given the national scope of Gramm-Leach-Bliley and state actions to implement its provisions, it is important that insurers have a consistent, uniform and workable regulatory scheme that provides meaningful information-sharing protections. Life insurers believe those provisions applicable to them in the Model regulation comprehensively provide that scheme.

We urge you to consider seriously Mr. Marshall's comments, and adopt this regulation in a form that provides both strong protections for a customer's personal health information and a regulatory framework the same or similar to that already adopted by a significant number of the states.

Thank you for the opportunity to comment on this most important proposal.

Sincerely,

Michael J. Bartholomew

April 16, 2002

Via E-mail and Overnight Delivery
psalvatore@state.pa.us

Original: 2257

Peter J. Salvatore
Regulatory Coordinator
Pennsylvania Insurance Department
1326 Strawberry Square
Harrisburg, PA 17120

Re: Privacy of Consumer Health Information – Proposed Rulemaking

Dear Mr. Salvatore:

Thank you for the opportunity to submit comments to the above referenced proposed regulation.

On behalf of Independence Blue Cross, ("IBC") set forth below are our general comments and specific concerns:

General Comments

Generally, IBC appreciates the Insurance Department's consideration of the comments previously submitted to the initial draft of the proposed regulation. The Department's intent to make the compliance date consistent with the compliance date of the HIPAA Privacy regulation will obviate the need for licensees to potentially abide with varying requirements for retaining the confidentiality of non-public health information.

Specific Concerns

Notwithstanding the foregoing general comments, IBC submits the following issues for consideration:

(1) Preamble – In the preamble it states that *"this proposed rulemaking is being promulgated to address several segments of the insurance industry that are not subject to the Federal Health Insurance Portability and Accountability Act (Federal HIPAA privacy regulation)"*. This regulation would, therefore, apply to entities such as third party administrators ("TPAs") that would be considered business associates not covered entities subject to the HIPAA privacy regulation. Is this the Department's intent?

(2) Section 1466.1(a)(3) – This section requires consent to disclose non-public personal health information although section 1466.11 requires an authorization for such disclosure.

Recommended Change:

Revise section 1466.1(a)(3) to delete "affirmative consent" and replace with "authorizations to be consistent with section 1466.11".

(3) Section 1466.2

- Definition of *Consumer* – Section 1466.2(G) suggests that the consumer would include TPAs as well as carriers. While PID certifies and regulates TPAs, TPAs as set forth above are business associates of group health plans and use or disclose protected health information ("PHI") at the direction of the group health plan. IBC is concerned that PID intends to enforce restrictions on TPAs that may be contrary to the wishes of a self-funded plan.

(4) Definition of *Health Care Provider* – Does this definition include all of the entities to whom a carrier may reimburse for the provision of services like DME suppliers. Under the definition provided, a DME supplier does not perform or provide specified health services or supplies consistent with the laws of the Commonwealth, or a health care facility.

(5) Definition of *Licensee* – Identical to the concerns raised previously, IBC does not believe that a licensee that administers a governmental health insurance program that is exempt under the proposed regulation should be bound to these requirements.

Recommended Change:

Delete subsection (D)(iv) under the definition of licensee. Revise subsection (B)(iii) to read:

(iii) – The term does not include governmental health insurance programs and those licensees that enroll, insure or otherwise provide an insurance related service to participants that procure health insurance through a governmental health insurance program exempted under subparagraph (iii).

(6) Section 1466.11 – Authorizations. To the extent the Department's intent is to mirror the HIPAA privacy regulations definition of payment and health care operations with the enumerated insurance functions, there are a few health insurance functions listed below that should be added to this exception.

- (11) – Amend to read: Disease Management and wellness programs
- (15) – Amend to read: Provider training, accreditation, certification, licensure and credentialing
- (33) – Add: Lawful reporting of disease, injury, vital statistics, child abuse, adult abuse, neglect or domestic violence.

(7) Section 1466.21 – Relationship with other laws. *Relationship with other state law or regulation.* This section of the proposed regulation would still require compliance with existing laws or regulations of the Commonwealth that relate to medical, records, health or insurance information privacy. To the extent that a licensee complies with the HIPAA privacy regulation, including the preemption provisions, a licensee should not be subject to this chapter. The HIPAA privacy regulation does not preempt more stringent state laws or regulations. Accordingly, section 1466.21(b) of the proposed regulation should be revised to read: "Nothing in this chapter preempts or supersedes more stringent laws or regulations of the Commonwealth that relate to medical records, health or insurance information privacy".

(8) Section 1466.23 – Violations. To the extent the PID is allowing licensees to opt for HIPAA compliance as set forth in section 1466.21(a), does the PID have to take statutory or regulatory authority action against licensees that violate HIPAA as well. For example, if HHS investigates a situation involving Licensee A and determines that Licensee A acted appropriately consistent with the HIPAA privacy regulation. Licensee A continues this business practice and a complaint is filed with the PID alleging that non-public personal health information was not properly disclosed. The PID could investigate the same situation and determine that Licensee A was not in compliance with the HIPAA privacy regulations and therefore, was required to obtain an individual's authorization under the proposed requirements. As a result, although the regulations appear to be the same with respect to use and disclosure of non-public health information, the interpretation of compliance by HHS and PID may be different and subject the licensee to penalties under the state Unfair Insurance Information Practice Act. IBC does not believe this is the intent of this provision and requests that it be revised to carve out 1466.21(a). This would thereby not subject licensees that comply with the Federal requirements including the preemption provisions to penalties under the state Unfair Insurance Information Practice Act.

IBC requests that PID take these comments into consideration as these proposed regulations are being put into final form. Should you have any questions, or would like to discuss any of these comments, please do not hesitate to contact Julie Haywood at (215) 241-9548.

Very truly yours,

Julie E. Haywood
Senior Counsel

JEH/fj

C: HIPAA Cross-Functional Team
Ken Fody
Jean Gorman

MANAGED CARE ASSOCIATION OF PENNSYLVANIA
240 North Third Street, Suite 501
P.O. Box 12108
Harrisburg, PA 17108-2108
e-mail: info@managedcarepa.org (717) 238-2600
website: www.managedcarepa.org Fax (717) 238-2656

Original: 2257

April 15, 2002

Mr. Peter J. Salvatore, Regulatory Coordinator
Pennsylvania Insurance Department
1326 Strawberry Square
Harrisburg, PA 17120

Via E-mail and U.S. Mail

RE: PROPOSED REGULATION – TITLE 31, CHAPTER 146b
PRIVACY OF CONSUMER HEALTH INFORMATION

Dear Mr. Salvatore:

On behalf of the member plans of the Managed Care Association of Pennsylvania (MCAP), I want to thank you for the opportunity to comment on the proposed regulation regarding the privacy of consumer health information. MCAP plans arrange for health care services for more than 1.4 million individuals through commercial, Medical Assistance and Medicare managed care plans.

We wish to thank the department for its effort in developing a regulation that would closely parallel that promulgated by the federal government for HIPAA. MCAP is also very appreciative of the department's endeavors to respond to the issues raised by MCAP in our comments of September 12, 2001 – most especially the effective date of the regulation which now corresponds to that of the federal legislation. Further, we note that the list of exceptions under Section 146.11(b) has been expanded to include subrogation and coordination of benefits under claims administration.

In our letter of September 12, 2001, MCAP raised a concern relative to plans forwarding information to their Primary Care Physician networks about patients who should have certain preventative services. Section 146(b)(33) includes preventative service reminders but they are qualified as those that *"do not require disclosure of nonpublic personal health information that a consumer has not previously disclosed directly to the recipient of the information"*. An example would be reminders to those physicians to perform foot

and eye examinations on diabetic patients. MCAP would recommend that this phrase be deleted from the final regulation. In cases where a member may change physicians, and that change has been processed in the plan's records, there is a possibility that the new physician would receive protected or identifiable information prior to the member's initial visit with the new doctor.

Again, we thank you for the opportunity to comment on this proposed regulation. Please do not hesitate to contact me at (717)238-2600 if you need additional information.

Sincerely,

Dolores M. Hodgkiss
Executive Director

PEOPLE BEFORE PROFITS

PANPHA

An Association of Nonprofit Senior Services

1100 Bent Creek Boulevard
Mechanicsburg, PA 17050

April 15, 2002

Peter J. Salvatore
Regulatory Coordinator
Insurance Department
1326 Strawberry Square
Harrisburg, PA 17120

Original: 2257

Dear Mr. Salvatore:

Thank you for meeting with Beth Greenberg and me to discuss PANPHA's concerns with the Insurance Department's proposed rule regarding Privacy of Consumer Health Information.

PANPHA is an association of 367 nonprofit providers of senior services in Pennsylvania. Most of the non-profit Continuing Care Retirement Communities (CCRCs) in the Commenwealth are members of PANPHA. We have three concerns about the proposed regulations.

- Since most CCRCs will need to comply with the Federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulation, it is our understanding that CCRCs will be exempt from the Insurance Department's Privacy of Consumer Health Information regulation because of Section 146b.21. Relationship with other laws. Is this the correct reading of this section?

- To the extent that the deadlines for compliance with HIPAA will be extended, we suggest that the compliance dates in Section 146b.24 be referenced to the date HIPAA compliance is implemented rather than giving a date. This will prevent facilities from having to comply with the state rule, then having to comply with HIPAA, if the HIPAA deadline is extended.

- To the extent that CCRCs may need to comply with the Department's rule rather than HIPAA, the 24-month limitation on the duration of authorization (Section 146b.12 Authorizations) will be problematic. We recommend that the authorization remain until the consumer is discharged.

Thank you for the opportunity to comment on the proposed rule regarding Privacy of

Consumer Health Information. If you have any questions, please contact Beth Greenberg at 717-763-5724 or beth@panpha.org.

Sincerely,

Christine F. Klejbuk

Christine F. Klejbuk
Vice President & Chief Public Policy Officer
chris@panpha.org

cc: Richard Sandusky, IRRC

HIGHMARK.

Kimberly S. Gray, Esq.
Chief Privacy Officer
(717) 730-1598
kimberly.gray@highmark.com

April 15, 2002

Original: 2257

Peter J. Salvatore, Regulatory Coordinator
Pennsylvania Insurance Department
1326 Strawberry Square
Harrisburg, PA 17120

Via e-mail: psalvatore@state.pa.us

RE: Proposed Rulemaking: Privacy of Consumer Health Information -- Title 31, Part VIII, Chapter 146b

Dear Mr. Salvatore:

I am writing on behalf of Highmark Inc. and its majority-owned and wholly-owned subsidiaries (Highmark) to which the above-referenced rulemaking regarding privacy of consumer health information (the "Draft Regulation") may be applicable.

As a major health care insurer and Medicare claims processor, Highmark provides health, dental, Medicare supplement, life, casualty and vision coverage, and has a vested interest in protecting the confidential information with which it is entrusted. Further, Highmark is interested in working to reduce administrative expenses and maintaining the availability and affordability of its products and services.

Highmark welcomes the attention demonstrated by the Pennsylvania Insurance Department in its promulgation of the Draft Regulation and commends the Department for its willingness to work with the health insurance industry in promulgating regulations protecting consumer health information.

Highmark, therefore, submits the following comment for consideration by the Insurance Department and further requests copies of other comments received by the Department regarding the Draft Regulation.

Compliance Date – §146b.24

Issue: By requiring compliance with the Draft Regulation on April 14, 2003 (or April 14, 2004, as the case may be), there is the potential for incongruity with the privacy rule promulgated on December 28, 2000 by the U.S. Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act of 1996, *65 Fed. Reg. 250, 82461-82510,* (the "Federal Regulation").

Recommendation/ Discussion: The compliance date of the Draft Regulation should be changed to mirror the Federal Regulation's compliance date. As the Federal Regulation now stands, this date is either April 14, 2003 or April 14, 2004, depending upon the amount of annual receipts. However, since there has been a Notice of Proposed Rulemaking offered which could modify the current Federal Regulation, and because HHS's determination as to enactment of the provisions this NPRM may take a significant amount of time, there may a movement to delay the compliance date of the Federal Regulation.

Additionally, we would suggest some clarification of the asset limits is in order, as an insurer with $5 million in assets would straddle both subsections of §146b.24 as it is now written.

Highmark believes that it would behoove the Department to modify §146b.24 as follows:

(a) **Licensees with more than $5 million in annual receipts shall comply with the applicable requirements of this chapter by the later of April 14, 2003, or such later time to which the compliance date of the Federal Regulation may be extended.**

(b) **Licensees with $5 million or less in annual receipts shall comply with the applicable requirements of this chapter by the later of April 14, 2004, or such later time to which the compliance date of the Federal Regulation may be extended.**

Thank you for this opportunity to provide comments on the Draft Regulation. If you have any questions regarding this communication, please direct questions to me by phone at (717) 730-1598 or by e-mail at kimberly.gray@highmark.com.

Sincerely,

Kimberly S. Gray, Esq.
Chief Privacy Officer

cc: Candy M. Gallaher
Douglas Reed
Thomas Wood, Esq.

Capital BlueCross

April 15, 2002

Mr. Peter J. Salvatore
Regulatory Coordinator
Pennsylvania Insurance Department
1326 Strawberry Square
Harrisburg, PA 17120

Original: 2257

Re: Comments on the Privacy of Consumer Health Information Draft Regulation

Dear Mr. Salvatore:

On behalf of Capital Blue Cross, I am providing you with our comments on the proposed regulation entitled *Privacy of Consumer Health Information* published in the March 16, 2002 edition of the Pennsylvania Bulletin.

We were very pleased to see the inclusion of the HIPAA deemer and compliance date provisions in sections §146b.21(a) and §146b.24(a) of the proposed regulation. We appreciate that the Insurance Department recognizes the significant effort many licensees are making to comply with the Federal Health Insurance Portability and Accountability Act Privacy rule and the tremendous burden that would result if licensees were required to comply with a second differing rule designed to provide individuals with similar protections.

We strongly support the retention of sections §146b.21(a) and §146b.24(a) in your final adoption of this regulation. We would however suggest one change which we believe will make the rule more workable. In recognition of the fact that the compliance date for the Federal regulation could change, as has already been the case with the HIPAA Transaction and Code Set extension, the following clarification would be helpful:

Section 146b.24 Compliance dates

(a) Licensees with $5 million or more in annual receipts shall comply with the applicable requirements of this chapter by *the final compliance date of the Federal regulation, which is currently set for April 14, 2003.*

(b) Licensees with $5 million or less in annual receipts shall comply with the applicable requirements of this chapter by *the final compliance date of the Federal regulation, which is currently set for* April 14, 2004.

We appreciate the opportunity to comment on this draft regulation. We also appreciate the reasonableness of the Insurance Department's approach to protecting the privacy of individuals' health information, especially in light of HIPAA Privacy.

If you or any of your staff have any questions about our comments, please do not hesitate to contact me by phone at (717) 541-6063 or e-mail at Kathy.Kelly@capbluecross.com.

Sincerely,

Kathleen P. Kelly
Privacy Officer

cc: P. Wong
A. Young
V. Carocci

Capital BlueCross

FAX TRANSMISSION SHEET

To Be Delivered Upon Receipt

This transmission, including the cover sheet, is 3 pages.

Please Deliver The Following Pages To:

Name: Peter Salvatore

Fax Number: 772-1969

Message: Comments on the Privacy of Consumer Health Information Draft Regulation

From: Kathy Kelly

Floor: 3rd Mail Drop: ____

Telephone Number: 541-6063

A return message, if required, should be faxed to (717) 541-6072.

Note: This communication may relate to coverages issued by or proposed to be issued by Capital Blue Cross (CBC) and/or its wholly owned subsidiary Capital Advantage Insurance Company (CAIC) and is being sent to you by CBC as the administrator of CBC and CAIC programs. CBC and CAIC are independent licensees of the Blue Cross and Blue Shield Association.

American Insurance Association

1130 Connecticut Ave. NW
Suite 1000
Washington, DC 20036
202-828-7100
Fax 202-293-1219
www.aiadc.org

April 15, 2002

BY E-MAIL

Original: 2257

Peter J. Salvatore
Regulatory Coordinator
Insurance Department
Commonwealth of Pennsylvania
1326 Strawberry Square
Harrisburg, PA 17120

RE: AIA Comments on Pennsylvania Draft Regulation (Spring 2002): Chapter 146b, "Privacy of Consumer Health Information"

Dear Mr. Salvatore:

The American Insurance Association ("AIA") is writing this letter in response to the most recent draft of the Pennsylvania regulation Chapter 146b, "Privacy of Consumer Health Information" ("Pennsylvania Health Privacy Regulation" or "Regulation"). AIA previously submitted comments on September 12, 2001 with respect to this Regulation, and many of the concerns outlined in those comments remain. We urge the Department to carefully consider the recommendations offered by AIA. For your convenience, we have attached a copy of the September 12 comments to this submission.

Our comments here focus on two issues of critical importance to AIA's member companies: (1) elimination of the "necessary" limitation on application of the business function exceptions; and (2) removal of the requirement in this Regulation that licensees obtain an agreement where a third party performs an excepted insurance function on behalf of the licensee. These items are discussed in further detail below.

§ 146b.11 (b) ("Necessary" Limitation)

Subsection 146b.11(b) states, "Nothing in this section prohibits, restricts or requires an authorization for the disclosure of nonpublic personal health information by a licensee to the extent that the disclosure of nonpublic personal health information is necessary for the performance of one or more of the following insurance functions by or on behalf of the licensee." (Emphasis added, highlighting the deviation from §17B of the NAIC Model Regulation.) This language generates a number of issues. First, the "necessary" limitation

has its origins in federal medical privacy regulations adopted by the U.S. Department of Health and Human Services ("HHS") that do not apply to the property/casualty industry. The Department should avoid language in state privacy regulations that has the effect of bringing property/casualty insurers into a federal privacy environment from which they have been intentionally excluded.

Second, the inclusion of this new standard separates the Pennsylvania Health Privacy Regulation from those of every other insurance regulatory jurisdiction that has adopted the NAIC Model Regulation's health information privacy article. As a result, property/casualty insurers will need to evaluate whether their existing privacy compliance programs – largely developed based on compliance with the NAIC Model Privacy Regulation – have to be altered to account for this additional standard. This in turn will require the devotion of unforeseen resources, and insurers doing business in Pennsylvania will incur increased costs. As AIA has stated repeatedly, uniformity and consistency of privacy regulation in the 51 insurance regulatory jurisdictions are crucial to implementing privacy standards in an efficient and effective manner.

Third, it is unclear who will determine what is "necessary" and how such a standard is to be consistently applied. Insurance licensees may be unable to predict how the Department applies the necessary limitation and whether perfectly acceptable information disclosure practices will be curtailed in Pennsylvania. An ambiguous and indefinable standard does not help regulators or the industry.

Fourth, it is unclear what purpose this additional language serves. Disclosures without authorization are already limited by the business function exceptions. Pennsylvania consumers will not be further protected by a quantity limitation on the amount of health information shared for an excepted business function.

For each of these reasons, as well as those contained in our September 12, 2001 submission, AIA respectfully urges the Department to remove the "necessary" limitation from § 146b.11 (b) of the Regulation.

§ 146b.11(c) ("Agreement" Requirement)

In § 146b.11(c), the Department has added a qualification to the business function exceptions outlined in § 146b.11(b) by requiring any such disclosures to third party non-licensees to be accompanied by an agreement "with the third party that prohibits the third party from disclosing or using the nonpublic personal health information for a purpose other than to carry out one or more of the insurance functions identified in subsection (b)." Not only is this a significant departure from Article V of the NAIC Model Privacy Regulation (which contains no similar requirement), it creates an impossible burden for Pennsylvania insurance licensees. If this section of the Health Regulation is adopted, licensees will need to enter into written confidentiality agreements with every unlicensed third party that handles nonpublic personal health information. Reading this provision literally, for example, a defense attorney engaged by a Pennsylvania insurer to represent the interests of the insurer and insured in an auto accident claim covered by an auto insurance policy would first need to sign a confidentiality agreement with the insurer before the attorney is permitted to review the insured's medical records. For each third party that handles personal information to perform

an excepted business function, the insurer would need to both execute a written agreement and be able to document and track the existence of every such agreement to the Department should it inquire. In addition, for every existing agreement, the insurer would need to establish a tracking mechanism. Such unanticipated additional hurdles add costs and delays in providing products and services without any added privacy protection to Pennsylvania consumers. We strongly urge the Department to delete this subsection from the Regulation.

It is possible that § 146b.11(c) represents an attempt to capture the elements of § 14(1)(b) of the NAIC Model Privacy Regulation, which provides an exception for joint marketing and third party service functions, but requires an agreement. However, this exception is only one of three alternative exceptions in the financial information provisions of the Model Regulation. The other two business function exception provisions (§§ 15 and 16) allow information disclosures by licensees to unlicensed third parties without the need for a separate agreement. All of the business function exceptions listed in §§ 15 and 16 of the Model Regulation are included in one form or another in § 146b.11(b) of the Regulation. As a result, it makes no sense to add an "agreement" condition.

Finally, § 146b.11(c) appears to be a backdoor mechanism for regulating the information sharing practices of non-licensees. The Department should not be establishing vicarious liability standards that make licensees responsible for the conduct of others.

In conclusion, on behalf of our member companies, AIA respectfully asks that the above comments, in tandem with comments submitted on September 12, 2001, be strongly considered when assessing revisions to the Pennsylvania Health Privacy Regulation. The recommendations submitted here are needed to make licensee compliance with the Regulation a manageable task. We reserve the right to supplement our comments as the process moves forward. Thank you for your attention. If you have questions or comments, please contact Taylor Cosby, Vice President, at 410-267-9581 or Stef Zielezienski, Assistant General Counsel, at 202-828-7175.

Respectfully submitted,

/s/ /s/

Taylor Cosby J. Stephen Zielezienski

The Insurance Federation of Pennsylvania, Inc.

1600 Market Street
Suite 1520
Philadelphia, PA 19103
Tel: (215) 665-0500 Fax: (215) 665-0540
E-mail: mailbox@ifpenn.org

Samuel R. Marshall
President & CEO

April 14, 2002

Original: 2257

Peter J. Salvatore
Regulatory Coordinator
Pennsylvania Insurance Department
Strawberry Square
Harrisburg, PA 17120

Re: Proposed Chapter 146b - Privacy of consumer health information

Dear Mr. Salvatore:

The Insurance Federation, on behalf of our member companies and in conjunction with our national counterparts, offers the following comments with respect to the Department's proposed regulation setting forth its privacy standards for insurers in possession of consumer health information.

At the outset, we note that insurers already have a strong record of protecting the privacy of consumers' health information, and the protections our industry already provides are consistent with those in this regulation. In that sense, we do not read this regulation as intended to bring an end to perceived or alleged insurer abuses of consumers' health privacy, but rather to codify protections already in place consistent with federal and national safeguards.

Our comments reflect this. They are, for the most part, requests for clarification and reasonableness in terms of compliance, as opposed to substantive objections to the underlying protections in the regulation.

That should not diminish the importance of the comments or the need to address our concerns. But we hope these comments are reviewed with the recognition that insurers

are just as committed to privacy as is the Department, with our concern being that the details in the regulation be clear and reasonable.

The importance of privacy should not diminish the importance of achieving it through a clear and reasonable regulation, and it should not be at the expense of accurate and efficient underwriting and claims administration - both of which are as important to consumers as is privacy. We therefore need to address, as much as possible, ambiguities in the regulation - not just to avoid future problems with the Department regarding compliance, but also to avoid disputes among insurers and between insurers and others on the precise requirements of the regulation.

Turning to the specifics of the regulation:

Section 146b.1 - Purpose

Section (a)(3): This subsection refers to consumer "consent," whereas the relevant sections in the regulation refer to "authorization." It also does not refer to the exceptions provided in the regulation.

Accordingly, we recommend this subsection be revised to read that this chapter "requires licensees to obtain the authorization of consumers prior to disclosing nonpublic personal health information, unless otherwise permitted herein."

Section 146b.2 - Definitions

"Consumer:" The inclusion of workers' compensation claimants raises several concerns. First is the concern raised by several national trade associations that workers compensation is not a form of insurance that is used for personal, family or household purposes and is therefore outside the Department's statutory authority.

Beyond this statutory authority concern, we have some concerns of practical implementation if workers compensation claimants

are to be included. We (and, I suspect, the Bureau of Workers Compensation) need clarity from the Insurance Department that nothing in this regulation is meant to alter the nature and means of sharing and disclosure of health information that presently occurs under the workers compensation system.

If the Department does envision that this regulation will require changes in this area, it should clarify precisely what that change is. Otherwise, we will be left with the prospect of violating one set of laws to satisfy another.

Our hope, of course, is that the Department does not envision that this regulation will require any changes in the sharing and disclosure of health information under the workers compensation system, and that it will clearly state this. In considering this issue, you should also consider that the workers compensation system is both insured and self-insured, and that claimants covered under self-insurance plans will not be consumers under this regulation. It makes no sense to have two sets of standards for claimants in that system, depending solely on the funding of their coverage.

"Health information:" This definition differs slightly, but perhaps significantly, from the "health information" definition in this regulation's companion subchapter, Chapter 146a covering privacy of consumers' financial information: This definition adds the exception of "nonpublic personal financial information."

We recommend deletion of this additional exception. As we read the definition of "nonpublic personal financial information," it specifically excludes "health information" through the exceptions listed in the definition of "personally identifiable financial information." Confusing as that seems, the net result is that health information is always an exception to financial information, not the other way around, as this definition would suggest.

Frankly, much of this problem could be resolved if the Department better clarifies two matters: First, that the financial privacy regulation does not apply to claims processing and similar insurance functions, but rather is

limited to information that might otherwise be used in marketing; and second, that the claims exemption applies to third party as well as first party claims (the New York Department issued a clarification on this on December 19, 2001).

In any event, if the Department regards the scope of the "health information" definitions in the two regulations as different, it should at least clarify those differences - and it should resolve any ambiguities as to what constitutes health versus financial information.

"Licensee:" We are not sure what other entities the Department envisions beyond insurers as defined in Section 201-A of the Insurance Department Act. For instance, that definition already includes agents and brokers, and HMOs - so there may be no need to also include them here as an addition to insurers. We recommend that this definition be revised consistent with the "insurer" definition in Section 201-A, and that it clarify the entities the Department intends to include beyond those in the Section 201-A definition.

Section 146b.11 - Required authorization and the "insurance function" exceptions

As a general comment, we recommend the Department clarify, either in the regulation itself or the preamble, that the authorization requirement is generally directed to marketing, not to underwriting, claims administration and other insurance functions. We also recommend the Department expressly include third party as well as first party claims within its claims exception - again, something that could be done in the preamble.

The Department may believe the regulation is already "abundantly clear" on this, as it asserted in its preamble to its financial privacy regulation. Unfortunately, not all insurers see this abundance in the text of the regulation or the Department's comment to date, and it has hampered the routine sharing of information in the claims context,

especially with respect to third party claims. As noted above, the New York Department issued this type of clarification on December 19, 2001; that may serve as helpful precedent.

Subsection (b) - Insurance function exception: We recommend the Department delete the phrase "to the extent that the disclosure of nonpublic personal health information is necessary." As the Department acknowledges, this phrase is not in Section 17(B) of the NAIC model on which this regulation is based; my understanding is that it is also not in any other state's regulation.

Our understanding of the insurance function exception, at least at the NAIC level and we hope in this regulation, is that it is intended to reflect and protect normal business operations of insurers.

The Department's "necessary" phrase is a dangerously ambiguous limitation to this, as "necessary" is a term that can vary among regulators and insurers. For instance, insurers might routinely disclose certain health information in underwriting or claims processing. But the Department could envision, with the perspective of hindsight review, some other way of performing those functions without disclosure and decree that the disclosure is therefore not necessary.

We appreciate the Department's contention that its addition of the "necessary" phrase is consistent with HIPAA. That federal standard, however, is itself vague, and it should not be perpetuated or compounded here - especially given that we have no assurance the Department will follow the same interpretations of "necessary" as will federal regulators.

In the alternative, the Department should at least clarify what it means by "necessary." To that end, if the Department is committed to incorporating a federal standard not found in any other state, we recommend it at least adopt the federal definition of "necessary" found in Section 509 of the GLBA. That section defines disclosures as being "necessary" if they are required, or are a "usual, appropriate or acceptable" method of performing the underlying function.

Subsections (b)(1) and (2): We appreciate that this language mirrors that of the NAIC model. We recommend, however, that the Department offer two clarifications in its preamble. First, the Department should clarify that these subsections apply to third party as well as first party claims (we also recommend the Department clarify the same with respect to its financial privacy regulation).

Second, the Department should clarify that this is a comprehensive inclusion of the claims process. For instance, claims investigation, negotiation and settlement are three routine claims functions that arguably might not fall within claims administration, adjustment and management. We appreciate that is not the result intended here; the Department should clarify this in its preamble.

Subsection (b)(23): We recommend the Department clarify that this includes reporting to various index and consumer reporting bureaus; again, this may be best done through the preamble.

Express acknowledgement of continued reporting to the various bureaus may also help resolve insurer anxiety about sharing information, whether financial or health, with respect to third party claims. Insurers routinely report this information on their claims to bureaus that is subsequently used by other insurers on their claims - thus essentially sharing information on third party as well as first party claims. Clarity on reporting to bureaus may therefore help achieve needed clarity within the industry on the sharing of information on third party claims.

Subsection (b)(31): This is another subsection where a seemingly minor variation from the NAIC model may cause unintended consequences. This subsection covers complying with court ordered warrants, subpoenas or summons issued by various officials. The NAIC model refers to complying with legal process, which suggests situations where information might be shared even in the absence of warrants, subpoenas or summons.

We recommend the Department add the NAIC language to the end of this subsection, stating "or otherwise comply with legal process."

Insurers are under increased pressure to be careful in the health and financial information they release, as evidenced by the October 26, 2001 ruling in Ingram v. Mutual of Omaha, F.Supp.2d (W.D.Mo. 2001) that we shared with you in our November 19, 2001 letter. The court in Ingram ruled that an insurer violated its fiduciary duty to its insured by releasing health information in response to a subpoena without objecting or moving to quash. Regulations such as this will not end the threat of such a ruling. But this regulation should not add to that threat - and this deviation from the NAIC model's reference to a "legal process" exception does just that.

Subsection (c) - Insurance functions performed by third parties on behalf of licensees: We recommend deletion, or significant revision, of this section. It requires that an insurer disclosing health information to a non-licensed third party "enter into an agreement" with a third party prohibiting the third party from disclosing the information for purposes beyond the insurance functions listed in section (b).

The section is not needed - probably the reason it was not included in the NAIC model. First, it should not apply to situations where the consumer has given authorization consistent with section (a) and Section 146b.12. This is really a drafting concern: While the heading in subsection (c) is limited to third parties handling areas covered by the insurance functions exceptions to the authorization requirement, the text here does not have that limit.

Second, it is not needed even if limited to the insurance functions exceptions in section (b). The insurer will be responsible to the Department if a third party acting on its behalf discloses information beyond those exceptions. After all, it is the insurer who is the licensed entity, and it is the insurer - not these non-licensed third parties - against whom the Department will proceed should the third parties go beyond the section (b) exceptions.

Requiring insurers to "enter into agreements" with their third party vendors adds only confusion, not security for consumers. The Department does not gain any enforcement power over the third party through this; if a third party violates an "agreement" with an insurer, the Department is still limited to going against the insurer.

Further, we are not sure what the Department means by an "agreement." Is this a contract? If so, this would impose a significant burden on insurers, for no gain in terms of privacy protection. It also raises a number of basic contractual concerns. For instance, what is the consideration; what is the damage to the insurer if the third party violates the contract?

Finally, we question the Department's statutory authority to do this. Insurers routinely use third parties to handle any number of insurance functions, many of which are regulated under Pennsylvania's insurance laws. We know of no other instance where the Department requires insurers to "enter into agreements" binding third parties to compliance with the insurance laws, and we do not believe the Department has the authority to do so here.

If the Department wants insurers to take affirmative steps to ensure that their vendors are aware of and comply with the limits of the insurance functions exceptions in section (b), it could require that insurers send out an annual notice of this to each of their vendors. That is a much simpler way of ensuring the goal of this section - that vendors be aware of the privacy limits in this regulation.

Section 146b.12 - Authorizations

Subsection (b) - Duration of authorization: We recommend the Department consider allowing authorizations to last for 30, not 24, months, at least for life insurers. A number of life insurers raised this problem because their incontestability periods last for 24 months; if something comes up at the end of the incontestability period, the insurer may need up to six months to resolve the problem.

This concern may be alleviated by clarifying that the exceptions authorization requirement are of unlimited duration, which I read as their intent. The difficulty is that life insurers tend to get authorizations even for some of the functions included in the "insurance functions" exceptions. Granted, they could begin limiting their authorizations. But that seems a penalty for providing more privacy than this regulation would require; the better solution is to extend their authorization period for 30 months.

Subsection (d): Record of authorization: We question the need for this subsection and its length. First, my admittedly quick review of the related financial privacy regulation and the "banks selling insurance" provisions in the Insurance Department Act does not uncover a similar record retention period for opt-out notices, essentially the financial equivalent of these authorizations. I am not sure why one is needed here.

Second, six years is too long; by way of example, the Department requires only three years for record retention of life illustrations, and I believe it requires records of complaints for a similar period.

As a practical matter, insurers will keep these records for some time to protect themselves from any consumer complaints. This regulation, however, applies only to dealings between the Department and insurers - and there is no need for the Department to go back six years in its review of insurers and any authorizations they receive.

Section 146b.24 - Compliance dates

The reference to "annual receipts" is confusing. We read this, from an insurer's perspective, to mean annual premiums, meaning that veritably all of our members will be subject to the proposed April 14, 2003 date - but the term "receipt" should be clarified to mean premium.

Further, we are not sure what this means for producers, who are also defined as "licensees" under this regulation. I am not sure a producer ever has "receipts," or even premiums, as he collects them only on behalf of an insurer. This could create an unintended loophole for producers to escape complinace with the

More important, we believe the April, 2003 compliance date is unreasonable unless the Department deletes the "agreement" requirement between insurers and third party vendors in Section 146b.11(c). If we are required to obtain separate agreements with every vendor acting on our behalf who might handle health information, it will take a period of time considerably longer than provided here.

As always, we appreciate the opportunity to comment on this, and we look forward to working with the Department and the IRRC to resolve these concerns and implement this regulation.

Sincerely,

Samuel R. Marshall