Regulatory Analysis Form

This space for use by IRRC

RECEIVED

2003 SEP 23 AM 9:47

INDEPENDENT REGULATORY REVIEW COMMISSION

(1) Agency

Insurance Department

(2) I.D. Number (Governor's Office Use)

11-215

IRRC Number: 2364

(3) Short Title

Standards for Safeguarding Customer Information

(4) PA Code Cite

31 Pa. Code, Chapter 146c, §§146c.1-146c.11

(5) Agency Contacts & Telephone Numbers

Primary Contact: Peter J. Salvatore, Regulatory Coordinator, 1326 Strawberry Square, Harrisburg, PA 17120, (717) 787-4429
Secondary Contact:

(6) Type of Rulemaking (check one)

☒ Proposed Rulemaking
☐ Final Order Adopting Regulation
☐ Final Order, Proposed Rulemaking Omitted

(7) Is a 120-Day Emergency Certification Attached?

☐ No
☐ Yes: By the Attorney General
☐ Yes: By the Governor

(8) Briefly explain the regulation in clear and nontechnical language.

The purpose of this proposed rulemaking is to adopt Chapter 146c in order to implement the remaining privacy requirements for nonpublic financial and health information set forth in Title V of the Gramm-Leach-Bliley Act (GLBA) (P.L. 102-106; 15 U.S.C. §§ 6801 et seq.) following the Department's implementation of Chapter 146a (Privacy of Consumer Financial Information) and Chapter 146b (Privacy of Consumer Health Information).

(9) State the statutory authority for the regulation and any relevant state or federal court decisions.

The proposal is made under the general rulemaking authority of §§ 205, 506, 1501 and 1502 of the Administrative Code of 1929 (71 P.S. §§ 66, 186, 411 and 412), and under the guidance of § 648 of The Insurance Department Act of 1921 (40 P.S. §§ 288), as amended by Act 40 of 1997 (P.L. 349, No. 40). Likewise, this proposal is made pursuant to the Department's rulemaking authority under the Unfair Insurance Practices Act (40 P.S. §§ 1171.1 et seq.) (as such authority is further explained in PALU v. Insurance Department, 371 A.2d 564 (Pa. Cmwlth. 1977)), because the Insurance Commissioner of the Commonwealth of Pennsylvania has determined that the improper disclosure and/or marketing of nonpublic personal financial and health information by members of the insurance industry constitutes an unfair method of competition and an unfair or deceptive act or practice.

(10) Is the regulation mandated by any federal or state law or court order, or federal regulation? If yes, cite the specific law, case or regulation, and any deadlines for action.

Title V of the Gramm-Leach-Bliley Act (GLBA) (P.L. 102-106; 15 U.S.C. §§ 6801 et seq.). The failure of a state to adopt such privacy regulations will result in the state's inability to override the federal insurance consumer protection regulations that were issued by the federal banking agencies in final form on December 4, 2000 pursuant to § 305 of the GLBA. See 65 Fed. Reg. 233, 75821.

(11) Explain the compelling public interest that justifies the regulation. What is the problem it addresses?

The Insurance Department seeks to amend Chapter 146c, §§146c.1-146c.11 because it is in the public interest to implement regulatory requirements recommended by the Federal Government on a statewide level in order to retain jurisdiction over certain insurance consumer protection areas involving banks selling insurance products.

(12) State the public health, safety, environmental or general welfare risks associated with nonregulation.

There are no public health, safety, environment or general welfare risks associated with this rulemaking.

(13) Describe who will benefit from the regulation. (Quantify the benefits as completely as possible and approximate the number of people who will benefit.)

The public will benefit from the regulation to the extent that it requires licensees of the Department to implement safeguards to protect insurance consumers' nonpublic personal health and financial information.

(14) Describe who will be adversely affected by the regulation. (Quantify the adverse effects as completely as possible and approximate the number of people who will be adversely affected.)

There will be no adverse effects on any party as a result of the amendment of this regulation.

(15) List the persons, groups or entities that will be required to comply with the regulation. (Approximate the number of people who will be required to comply.)

The regulation applies to all licensees doing the business of insurance in the Commonwealth, unless specifically exempted from the requirements of the regulation.

(16) Describe the communications with and input from the public in the development and drafting of the regulation. List the persons and/or groups who were involved, if applicable.

Comments regarding this proposed regulation were solicited from the various trade associations representing the insurance industry. The Department received comments from the following industry members and trade associations: the American Insurance Association ("AIA"), the Alliance of American Insurers ("AAI"), Independence Blue Cross ("IBC"), Capital Blue Cross ("CBC"), the American Council of Life Insurers ("ACLI"), the Insurance Federation of Pennsylvania ("IFP"), and Highmark, Inc. ("Highmark").

(17) Provide a specific estimate of the costs and/or savings to the regulated community associated with compliance, including any legal, accounting or consulting procedures, which may be required.

This proposed regulation will not have any impact on costs associated with the Department's licensees or the public.

(18) Provide a specific estimate of the costs and/or savings to local governments associated with compliance, including any legal, accounting or consulting procedures, which may be required.

There are no costs or savings to local governments associated with this rulemaking.

(19) Provide a specific estimate of the costs and/or savings to state government associated with the implementation of the regulation, including any legal, accounting, or consulting procedures, which may be required.

There are no costs or savings associated to state government associated with this rulemaking.

Regulatory Analysis Form

(20) In the table below, provide an estimate of the fiscal savings and costs associated with implementation and compliance for the regulated community, local government, and state government for the current year and five subsequent years. N/A

	Current FY Year	FY +1 Year	FY +2 Year	FY +3 Year	FY +4 Year	FY +5 Year
SAVINGS:	**$**	**$**	**$**	**$**	**$**	**$**
Regulated Community						
Local Government						
State Government						
Total Savings						
COSTS:						
Regulated Community						
Local Government						
State Government						
Total Costs						
REVENUE LOSSES:						
Regulated Community						
Local Government						
State Government						
Total Revenue Losses						

(20a) Explain how the cost estimates listed above were derived.

N/A.

Regulatory Analysis Form

(20b) Provide the past three-year expenditure history for programs affected by the regulation.
N/A.

Program	FY –3	FY -2	FY -1	Current FY

(21) Using the cost-benefit information provided above, explain how the benefits of the regulation outweigh the adverse effects and costs.

No costs or adverse effects are anticipated as a result of this regulation.

(22) Describe the nonregulatory alternatives considered and the costs associated with those alternatives. Provide the reasons for their dismissal.

Amending Chapter 146c, §§146c.1-146c.11 to implement the NAIC Model regulation is the most efficient method to achieve consistency among the states. No other alternatives were considered.

(23) Describe alternative regulatory schemes considered and the costs associated with those schemes. Provide the reasons for their dismissal.

No other regulatory schemes were considered. This proposed regulation is the most efficient method of updating the regulatory requirements.

(24) Are there any provisions that are more stringent than federal standards? If yes, identify the specific provisions and the compelling Pennsylvania interest that demands stronger regulation.

No.

(25) How does this regulation compare with those of other states? Will the regulation put Pennsylvania at a competitive disadvantage with other states?

The rulemaking will not put Pennsylvania at a competitive disadvantage with other states. It merely provides for consistency with the GLBA.

(26) Will the regulation affect existing or proposed regulations of the promulgating agency or other state agencies? If yes, explain and provide specific citations.

No.

(27) Will any public hearings or informational meetings be scheduled? Please provide the dates, times, and locations, if available.

No public hearings or informational meetings are anticipated.

Regulatory Analysis Form
(28) Will the regulation change existing reporting, record keeping, or other paperwork requirements? Describe the changes and attach copies of forms or reports, which will be required as a result of implementation, if available. The promulgation of this regulation may impose some additional paperwork requirements on the Department, insurers, licensees, or the general public. However, this paperwork would be mandated by the Federal government if not regulated by the Commonwealth.
(29) Please list any special provisions which have been developed to meet the particular needs of affected groups or persons including, but not limited to, minorities, elderly, small businesses, and farmers. The rulemaking will have no effect on special needs of affected parties.
(30) What is the anticipated effective date of the regulation; the date by which compliance with the regulation will be required; and the date by which any required permits, licenses or other approvals must be obtained? The rulemaking will undergo a 30-day public comment period and will take effect upon approval of the final form regulation by the legislative standing committees, the Office of the Attorney General, and the Independent Regulatory Review Commission and upon final publication in the *Pennsylvania Bulletin.*
(31) Provide the schedule for continual review of the regulation. The Department reviews each of its regulations for continued effectiveness on a triennial basis.

CDL-1

FACE SHEET FOR FILING DOCUMENTS WITH THE LEGISLATIVE REFERENCE BUREAU

(Pursuant to Commonwealth Documents Law)

RECEIVED
2003 SEP 23 AM 9:47
INDEPENDENT REGULATORY REVIEW COMMISSION

#2364

DO NOT WRITE IN THIS SPACE

Copy below is hereby approved as to form and legality. Attorney General

By: _____
(Deputy Attorney General)

SEP 10 2003
Date of Approval

→ Check if applicable. Copy not approved. Objections attached.

Copy below is hereby certified to be a true and correct copy of a document issued, prescribed or promulgated by:

Insurance Department
(AGENCY)

DOCUMENT/FISCAL NOTE NO. 11-215

DATE OF ADOPTION: _____

BY: M. Diane Koken
M. Diane Koken
Insurance Commissioner

TITLE: _____
(EXECUTIVE OFFICER, CHAIRMAN OR SECRETARY)

Copy below is hereby approved as to form and legality. Executive or Independent Agencies

BY: Tanya C. Hubbs

8/18/03
DATE OF APPROVAL

Assistant (~~DEPUTY~~ GENERAL COUNSEL)
(~~CHIEF COUNSEL, INDEPENDENT AGENCY~~)
(STRIKE INAPPLICABLE TITLE)

→ Check if applicable. No Attorney General approval or objection within 30 days after submission.

NOTICE OF PROPOSED RULEMAKING

INSURANCE DEPARTMENT

31 Pa. Code, Chapter 146c
§§ 146c.1-146c.11

Standards for Safeguarding Customer Information

Preamble

The Insurance Department (Department) proposes to adopt, 31 Pa. Code, Chapter 146c, Standards for Safeguarding Customer Information, §§ 146c.1-146c.11, to read as set forth in Annex A. The proposal is made under the general rulemaking authority of §§ 205, 506, 1501 and 1502 of the Administrative Code of 1929 (71 P.S. §§ 66, 186, 411 and 412), and under the guidance of § 648 of The Insurance Department Act of 1921 (40 P.S. §§ 288), as amended by Act 40 of 1997 (P.L. 349, No. 40). Likewise, this proposal is made pursuant to the Department's rulemaking authority under the Unfair Insurance Practices Act (40 P.S. §§ 1171.1 et seq.) (as such authority is further explained in PALU v. Insurance Department, 371 A.2d 564 (Pa. Cmwlth. 1977)), because the Insurance Commissioner of the Commonwealth of Pennsylvania has determined that the improper disclosure and/or marketing of nonpublic personal financial and health information by members of the insurance industry constitutes an unfair method of competition and an unfair or deceptive act or practice.

Purpose

The purpose of this proposed rulemaking is to adopt Chapter 146c in order to implement the remaining privacy requirements for nonpublic financial and health information set forth in Title V of the Gramm-Leach-Bliley Act (GLBA) (P.L. 102-106; 15 U.S.C. §§ 6801 et seq.) following the Department's implementation of Chapter 146a (Privacy of Consumer Financial Information) and Chapter 146b (Privacy of Consumer Health Information).

Title V of GLBA requires various state and federal regulators of the financial services industries to promulgate regulations for their respective regulated communities. For example, state insurance authorities are required by Title V of the GLBA to establish appropriate consumer privacy standards for various entities in the insurance industry. The failure of a state to adopt such privacy regulations will result in the state's inability to override the federal insurance consumer protection regulations that were issued by the federal banking agencies in final form on December 4, 2000 pursuant to § 305 of the GLBA. See 65 Fed. Reg. 233, 75821 (to be codified at 12 C.F.R. Parts 14, 208, 343 and 536). These regulations became effective on April 1, 2001, and they pertain generally to the sale of insurance by financial institutions and specifically to such matters as referral fees, separation of banking and insurance sales areas and disclosures regarding the nature of insurance products that are sold by banks.

The Department has already promulgated Chapter 146a (Privacy of Consumer Financial Information) and Chapter 146b (Privacy of Consumer Health Information), which were based upon the National Association of Insurance Commissioners Model Privacy of Consumer Financial and Health Information Regulation. With regard to health information, the Privacy of Consumer Health Information regulation generally requires that licensees of the Department obtain an authorization from a consumer prior to disclosing nonpublic personal health information unless the disclosure is specifically excluded from the requirements of the regulation. The Privacy of Consumer Financial Information Regulation requires that licensees provide consumers with notice and an opportunity to "opt out" of disclosures of their nonpublic personal financial information prior to making such disclosures. The purpose of this proposed

rulemaking is to implement the remaining requirements of Title V relating to the internal safeguarding of customer information maintained by a licensee. Accordingly, this proposal is based upon the NAIC Standards for Safeguarding Customer Information Model Regulation. For purposes of Committee review and IRRC review, a copy of said Model Regulation is attached.

Explanation of Regulatory Changes and Pre-Proposed Comments and Responses

On November 9, 2002, the Department published in the *Pennsylvania Bulletin* an Advanced Notice of Proposed Rulemaking for its Standards for Safeguarding Customer Information Regulation ("privacy standards regulation") soliciting comments from the insurance industry. See 32 Pa.B. 5595 (November 9, 2002). The Department received comments from the following industry members and trade associations: the American Insurance Association ("AIA"), the Alliance of American Insurers ("AAI"), Independence Blue Cross ("IBC"), Capital Blue Cross ("CBC"), the American Council of Life Insurers ("ACLI"), the Insurance Federation of Pennsylvania ("IFP"), and Highmark, Inc. ("Highmark"). The following is a summary of those comments as well as the Department's reaction thereto.

Section 146c.1 (relating to purpose) explains that the purpose of the regulation is to establish standards to guide licensees of the Department in the development and implementation of administrative, technical and physical safeguards that protect the security, confidentiality and integrity of customer information, and protect against any anticipated threats or hazards to the security or integrity of customer records. The standards also are intended to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

Paragraph 3 of §146c.1 states that one of the purposes of the privacy standards regulation is to protect against any anticipated threats or hazards to the security or integrity of customer records maintained by licensees. Highmark believes that the standard in this section is unattainable because it would be impossible for a licensee to protect against **any** anticipated threats or hazards to the security or integrity of customer information. Accordingly, Highmark recommends that the word "reasonably" be inserted after the word "any" in paragraph 3 of this section in order to make the standard more objective and attainable. The Department has adopted Highmark's recommendations in its proposed rulemaking.

Section 146c.2 (relating to definitions) defines the terms that are relevant to this chapter.

AAI and AIA commented that the definition of "customer" in the regulation is overly broad because it encompasses both "consumers" and "customers" as defined in the health and financial privacy regulations. AAI asserted that this requirement goes beyond the requirements of the GLBA and, therefore, the Department lacks statutory authority to extend the scope of the regulation. See 15 U.S.C. § 6801(b). The Department respectfully disagrees with the comments from AAI and AIA because the Department does not rely on the GLBA for its statutory authority for the promulgation of this regulation. Instead, the Department relies upon its implied rulemaking authority granted by the Unfair Insurance Practices Act ("UIPA"), 40 P.S. §§ 1171.1 – 1171.15. See PALU v. Insurance Department, 371 A.2d 564 (Pa. Cmwlth. 1977).

Furthermore, the GLBA merely establishes a floor for the regulation of insurance privacy, and the law explicitly states that insurance regulators are permitted to be more protective of insurance information privacy. Accordingly, the comments made by AAI and AIA pertaining to the definition of "customer" in the privacy standards regulation are misplaced, and no modifications have been made to the definition in this proposed regulation.

Section 146c.3 (relating to information security program) requires licensees to implement a comprehensive written information security program appropriate to the size and complexity of the licensee and the nature and scope of its activities. The information security program must include administrative, technical and physical safeguards for the protection of customer information.

Section 146c.4 (relating to objectives of information security program) explains that a licensee's information security program should be designed to do the following: (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of the information; and (3) protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Section 146c.4 of the privacy standards regulation identifies the objectives of the information security programs required by the regulation, one of which is to ensure the security and confidentiality of customer information. Highmark commented that the use of the word "ensure" in paragraph 1 of this section imposes an unreasonable standard upon licensees because the term means to "promise, guarantee or pledge." Accordingly, Highmark recommends that the word "safeguard" be used instead of the word "ensure." The Department agrees with this comment and has made an appropriate change in the proposed regulation.

Another objective of an information security program is identified in paragraph 2 of §146c.4, which states that an information security program must be designed to protect against any anticipated threats or hazards to the security or integrity of customer information. As in its comment pertaining to §146c.1, Highmark believes that the standard in this section is unattainable because it would be impossible for a licensee to protect against **any** anticipated threats or hazards. Therefore, Highmark recommends that the word "reasonably" be inserted after the word "any" in paragraph 2 of this section in order to make the standard more objective and attainable. The Department is in agreement with the comment provided by Highmark and has modified its proposed rulemaking to incorporate Highmark's suggestion.

Section 146c.5 (relating to examples of methods of development and implementation) explains that the actions and procedures found in §§146c.6 through 146c.9 of this chapter are examples of the methods of implementation found in the requirements at §§146c.3 and 146c.4 and are not the exclusive methods that licensees can comply with this chapter.

This provision of the privacy standard regulation states that the examples in §§146c.6 through 146c.9 of actions and procedures that comply with the information security program requirements are merely non-exclusive illustrations that licensees may follow when

implementing an information security program. In their comments, AIA requested that §146c.5 (as well as §§146c.6 through 146c.9) be deleted because they believe that the examples create the appearance of a standard that all companies must follow, and this perception might result in additional litigation against licensees. The Department has not adopted the recommendation of AIA because the compliance examples provide invaluable guidance to licensees as they develop and implement information security programs to protect the security and integrity of customer information. Furthermore, the prefatory language in §146c.5 makes it abundantly clear that the examples in the regulation are non-exclusive and are for illustrative purposes only.

Section 146c.6 (relating to assessing risk) provides examples where the licensee identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems. This section also provides examples relating to how a licensee may assess the likelihood and potential damage of these threats and assess the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Section 146c.7 (relating to managing and control risk) provides examples of how a licensee may comply with this chapter by designing its information security program to: (1) control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities; (2) train staff, as appropriate, to implement the licensee's information security program; and (3) regularly test or otherwise regularly monitor the key controls, systems and procedures of the information security program.

Section 146c.8 (relating to overseeing service provider arrangements) provides examples of how a licensee may comply with this chapter by exercising appropriate due diligence in selecting its service providers, requiring its service providers to implement appropriate measures designed to meet the objectives of this regulation, and by taking appropriate steps to confirm that its service providers have satisfied these obligations.

Several comments focused on the compliance example in §146c.8, which addresses how a licensee may comply with the regulation by including certain safeguards when a third party service provider receives or maintains customer information on behalf of a licensee. The comments are also directed towards a provision in the Department's health privacy regulation, stating that licensees may be held liable for illegal disclosures of health information by its third party service providers. See 31 Pa. Code §146b.11(d). Several commentators, including the ACLI and the IFP, recommended that the regulation incorporate the standards found in the final federal data security regulation issued by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act ("federal regulation"). The federal regulation was adopted in final form on February 20, 2003.

Based upon the concerns presented by the industry, the Department has adopted a standard that is similar to that found in the federal regulation. However, the additional language has been included in the regulation as §146c.10(b). The Department believes that this additional provision satisfies the concerns of the commentators, while remaining consistent with the principles of the

UIPA in that it requires a pattern or practice and it utilizes the "knew or reasonably should have known" standard.

Section 146c.9 (relating to adjusting the program) provides examples of compliance with this chapter where the licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

Section 146c.10 (relating to violations) describes that violations of this chapter are deemed and defined by the Commissioner to be an unfair method of competition and an unfair or deceptive act or practice and shall be subject to any applicable penalties or remedies contained in the Unfair Insurance Practices Act (40 P.S. §§1171.1-1171.15).

Section 146c.10 provides that a violation of the privacy standards regulation is deemed and defined to be an "unfair method of competition" and an "unfair or deceptive act or practice," subject to the penalties and remedies of the UIPA. This language is taken verbatim from the Department's previous financial and health privacy regulations. See 31 Pa. Code §§146a.43 and 146b.23. Highmark suggested that a licensee should be held liable only when it "knew or should have known" that its actions were in violation of the regulation. AAI is concerned that creating new unfair insurance practices encourages private litigation and the resulting expenses would be burdensome. AIA recommended a clarification that violations of only §146c.3 or §146c.4 will result in a violation of the regulation since the remaining sections are definitions and examples for compliance.

The Department has not adopted Highmark's proposed modifications because §146c.10 is taken verbatim from the financial and health privacy regulations and a substantive modification to the violation provision in this regulation might implicate the language in the Department's two prior privacy regulations. Likewise, the Department disagrees with AAI's comment because there is no private cause of action for violations of the UIPA. See Smith v. Nationwide Mut. Fire Ins. Co., 935 F. Supp 616 (W.D. Pa. 1996), D'Ambrosio v. Penn. Nat. Mut. Cas. Ins. Co., 431 A.2d 966 (Pa. 1981).

However, the recommendation of AIA might provide additional clarity to the regulation and further reinforce that the examples in §§146c.5 though 146c.9 are only illustrative examples of compliant actions and procedures that licensees may utilize in the development and implementation of an information security program. Accordingly, the Department has amended its proposed regulation to adopt the suggestion provided by AIA.

Section 146c.11 (relating to effective date) gives the parameters as to when this chapter will become effective.

Highmark, IBC and CBC suggested that the effective date of the regulation should mirror that of the federal regulation, which is April 20, 2005 for large health plans and April 20, 2006 for

small health plans. See 45 C.F.R. § 164.318(a). AAI suggests that insurers need at least 6 months to comply with the regulation, so the effective date should be extended in the proposed regulation.

The Department has not mirrored the compliance date for the federal regulation in this proposed rulemaking because compliance with that regulation will not be enforced for more than two years. However, because implementation of the information security programs by the licensees will likely take some time, the Department has extended the compliance date for this proposed regulation to six months after the promulgation of the regulation in final form.

Compliance with the federal regulation.

Because the final federal regulation includes requirements similar to those in the Department's privacy standards regulation, several comments requested that licensees be able to comply only with the federal regulation and be deemed compliant with the Department's regulation. Specifically, Highmark and CBC would like the Department to include a deemer provision similar to that in the health privacy regulation whereby if a licensee is compliant with the federal regulation, then it is deemed compliant with the privacy standards regulation.

It is true that the federal regulation and the Department's privacy standards regulation have some overlapping requirements, and it is further true that the requirements of the Department's regulation are not inconsistent with those in the federal regulation. Therefore, if a licensee satisfies the requirements of the federal regulation, the licensee would also likely satisfy many of the requirements of the Department's regulation. However, compliance with the federal regulation will not satisfy all of the requirements of the Department's regulation because the federal regulation only addresses health information and not financial information. Therefore, if a deemer provision is included and a licensee complies with the federal regulation, that licensee would be able to avoid the information security requirements for financial information. Accordingly, the requested deemer provision has not been included in the proposed regulation.

Fiscal Impact

There is no anticipated fiscal impact as a result of the proposed rulemaking. Insurers need to comply with the Gramm-Leach-Bliley Act and 31 Pa. Code, §§146a.1-146a.44 (relating to Privacy of Consumer Financial Information) and §§146b.1-146b.24 (relating to Privacy of Consumer Health Information). Therefore, most, if not all, of the methods should be in place. This Chapter bridges any gaps in those regulations and the privacy of consumer information.

Paperwork

There is no anticipated additional paperwork expected as a result of this rulemaking.

Affected Parties

The proposed rulemaking will affect all licensed insurers doing the business of insurance in this Commonwealth.

Effectiveness/Sunset Date

The rulemaking will become effective _____ (Editor's Note: the rulemaking will become effective by the first of the month following 180 days from the publication date of this regulation in final form.)

Contact Person

Questions or comments regarding the proposed rulemaking may be addressed in writing to Peter J. Salvatore, Regulatory Coordinator, Insurance Department, 1326 Strawberry Square, Harrisburg, PA 17120, within 30 days following the publication of this notice in the *Pennsylvania Bulletin*. Questions and comments may also be e-mailed to *psalvatore@state.pa.us* or faxed to (717) 772-1969.

Pursuant to the Regulatory Review Act (71 P.S. §745 et seq.), the Department is required to write to all commentators, requesting whether or not they wish to receive a copy of the final form regulation. In order to better serve our stakeholders, the Department has made a determination that all commentators will receive a copy of the final form rulemaking when it is made available to the IRRC and the Legislative Standing Committees.

Regulatory Review

Under section 5(a) of the Regulatory Review Act (71 P.S. §745.5(a)), on September 23, 2003, the Department submitted a copy of this proposed rulemaking to the Independent Regulatory Review Commission (IRRC) and to the Chairpersons of the Senate Banking and Insurance Committee and the House Insurance Committee. In addition to the submitted proposed rulemaking, the Department has, as required by the Regulatory Review Act, provided IRRC and the Committees with a copy of a detailed Regulatory Analysis Form prepared by the Department. A copy of that material is available to the public upon request.

The IRRC will notify the Department of any objections to any portion of the proposed rulemaking within 30 days of the close of the public comment period. The notification shall specify the regulatory review criteria that have not been met by that portion. The Regulatory Review Act specifies detailed procedures for the Department, the Governor, and the General Assembly to review these objections before final publication of the regulations.

M. DIANE KOKEN
Insurance Commissioner

Annex A

TITLE 31. INSURANCE. PART VIII. MISCELLANEOUS PROVISIONS. Chapter 146c. Standards for Safeguarding Customer Information.

Sec.

§ 146c.1. Purpose.

This regulation establishes standards:

(1) For developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.

(2) For ensuring the security and confidentiality of customer records and information.

(3) To protect against any reasonably anticipated threats or hazards to the security or integrity of such records.

(4) To protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

(5) That shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

§ 146c.2. Definitions.

The following words and terms, when used in this chapter, have the following meanings, unless the context clearly indicates otherwise:

Act--The Insurance Department Act of 1921 (40 P. S. §§ 1--321)

Customer—Either a "consumer" or "customer" as defined in section 2 of chapter 146a of the Department's regulations (31 Pa.Code § 146a.2) or a "consumer" as defined in section 2 of chapter 146b of the Department's regulations (31 Pa.Code § 146b.2).

Customer information – Either "nonpublic personal financial information" as defined in section 2 of chapter 146a of the Department's regulations (31 Pa.Code § 146a.2) or "nonpublic personal health information" as defined in section 2 of chapter 146b of the Department's regulations (31 Pa.Code § 146b.2) about a customer, whether in paper, electronic or other form that is maintained by or on behalf of the licensee.

Customer information systems - The electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

Department -- The Insurance Department of the Commonwealth.

Licensee –As defined in either section 2 of chapter 146a of the Department's regulations (31 Pa.Code § 146a.2) or section 2 of the chapter 146b of the Department's regulations (31 Pa.Code § 146b.2), except that the term shall not include a purchasing group or a nonadmitted

insurer in regard to the surplus lines business conducted pursuant to 40 P.S. §§ 991.1601-991.1625.

Service provider - A person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

§146c.3. Information security program.

Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

§146c.4. Objectives of information security program.

A licensee's information security program shall be designed to do each of the following:

(1) Safeguard the security and confidentiality of customer information.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of the information.

(3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

§146c.5. Examples of methods of development and implementation.

The actions and procedures described in §§ 146c.6 through 146c.9 of this chapter are examples of methods of implementation of the requirements of §§146c.3 and 146c.4 of this

chapter. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement §§146c.3 and 146c.4 of this chapter.

§146c.6. Assess risk.

The licensee:

(1) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.

(2) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

(3) Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

§146c.7. Manage and control risk.

The licensee:

(1) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities.

(2) Trains staff, as appropriate, to implement the licensee's information security program.

(3) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

§146c.8. Oversee service provider arrangements.

The licensee:

(1) Exercises appropriate due diligence in selecting its service providers.

(2) Requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

§146c.9. Adjust the program.

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

§146c.10. Determined violation.

(a) Violations of sections 146c.3 and 146c.4 of this chapter are deemed and defined by the Commissioner to be an unfair method of competition and an unfair or deceptive act or practice and shall be subject to any applicable penalties or remedies contained in the Unfair Insurance Practices Act (40 P.S. §§1171.1-1171.15).

(b) A licensee has violated this chapter when the licensee knew or reasonably should have known of a pattern of activity or a practice of a service provider that constitutes either a violation

of Chapter 146a, Chapter 146b or this chapter or a material breach of the contract or other arrangement between the licensee and the service provider, unless the licensee took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, did the following:

(1) Terminated the contract or arrangement with the service provider, if feasible.

(2) If termination is not feasible, reported the violation or breach to the department.

§146c.11. Effective date.

Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this regulation within six months from the publication date of this regulation in final form.

COMMONWEALTH OF PENNSYLVANIA
INSURANCE DEPARTMENT
SPECIAL PROJECTS OFFICE
1326 Strawberry Square
Harrisburg, PA 17120

Phone: (717) 787-4429
Fax: (717) 772-1969
E-mail: psalvatore@state.pa.us

September 23, 2003

Mr. Robert Nyce
Executive Director
Independent Regulatory Review Comm.
333 Market Street
Harrisburg, PA 17101

Re: Insurance Department Proposed Regulation No. 11-215, Standards for Safeguarding Customer Information

Dear Mr. Nyce:

Pursuant to Section 5(a) of the Regulatory Review Act, enclosed for your information and review is proposed regulation 31 Pa. Code, Chapter 146c, Standards for Safeguarding Customer Information.

The purpose of this proposed rulemaking is to adopt Chapter 146c in order to implement the remaining privacy requirements for nonpublic financial and health information set forth in Title V of the Gramm-Leach-Bliley Act (GLBA) (P.L. 102-106; 15 U.S.C. §§ 6801 et seq.) following the Department's implementation of Chapter 146a (Privacy of Consumer Financial Information) and Chapter 146b (Privacy of Consumer Health Information).

If you have any questions regarding this matter, please contact me at (717) 787-4429.

Sincerely yours,

Peter J. Salvatore
Regulatory Coordinator

11-215p.doc

TRANSMITTAL SHEET FOR REGULATIONS SUBJECT TO THE REGULATORY REVIEW ACT

I.D. NUMBER:	11-215
SUBJECT:	Standards for Safeguarding Customer Information
AGENCY:	DEPARTMENT OF INSURANCE

TYPE OF REGULATION

X Proposed Regulation

Final Regulation

Final Regulation with Notice of Proposed Rulemaking Omitted

120-day Emergency Certification of the Attorney General

120-day Emergency Certification of the Governor

Delivery of Tolled Regulation
a. With Revisions b. Without Revisions

RECEIVED
2003 SEP 23 AM 9:47
INDEPENDENT REGULATORY REVIEW COMMISSION

FILING OF REGULATION

DATE	SIGNATURE	DESIGNATION
9/23/03	D. Stephagen	HOUSE COMMITTEE ON INSURANCE
9/23/03	M E Mitchell	
9/23/03	J. D. Timmer	SENATE COMMITTEE ON BANKING & INSURANCE
9/23/03	T. McDaniel	
9/23/03	E. Pagán	INDEPENDENT REGULATORY REVIEW COMMISSION
		ATTORNEY GENERAL (for Final Omitted only)
9/23/03	Maya Bacas	LEGISLATIVE REFERENCE BUREAU (for Proposed only)

September 15, 2003