



**BlueCross BlueShield
Association**

An Association of
Independent Blue Cross
and Blue Shield Plans

1310 G Street, N.W.
Washington, D.C. 20005
Telephone 202.626.4780
Fax 202.626.4833



March 31, 2000

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th and C Streets, NW
Washington, DC 20551

Re: Docket No. R-1058

Dear Ms. Johnson:

I am writing to submit the Blue Cross and Blue Shield Association comments regarding the proposed privacy rule published pursuant to the Gramm-Leach-Bliley Act (GLB) on privacy of consumer financial information (12 CFR Part 216, Docket No. R-1058). The Blue Cross and Blue Shield Association (BCBSA) represents 49 independent Blue Cross and Blue Shield (BCBS) Plans across the country, covering 75 million Americans.

We understand that the recently proposed GLB privacy rules do not directly apply to Blue Cross and Blue Shield Plans. However, BCBSA is submitting comments because the federal GLB privacy rules will likely be used as a baseline or precedent for future privacy laws and regulations adopted by the states.

For BCBS Plans, there is no question as to *whether* patient records should be kept confidential, but only as to *how* this should be accomplished. We look forward to working with the Board of Governors of the Federal Reserve System (Board), as well as the Department of Health and Human Services (HHS) and other federal agencies, to implement practical and uniform privacy protections that facilitate quality assurance efforts and the timely payment for health care services.

Our over-riding concern with the GLB proposed privacy rules is that their substantial overlap with other federal privacy rules as well as state regulations will create a confusing patchwork of rules for consumers and insurers.

States already have a myriad of privacy laws and regulations dealing with patient records. In addition, the Department of Health and Human Services (HHS) has recently issued two very comprehensive proposed rules related to privacy and security under the direction of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HHS expects to issue final versions of these rules, as well as additional proposed rules on privacy, in the near future.

The GLB proposed regulation not only duplicates sections of the HHS proposed rule on privacy, but also includes conflicting rules. Such duplication and conflict will make it very difficult to comply with the two regulations, and would impair the cost-saving goals of HIPAA's administrative simplification provisions. Moreover, the overlap and complexity of the federal rules creates a potential market disincentive – making it difficult

for health insurers to meaningfully interact with the financial services industry. This would defeat the underlying spirit of the Gramm-Leach-Bliley Act.

To alleviate confusion and minimize costs, BCBSA recommends that health insurers that are subject to the HIPAA privacy rules be deemed in compliance with the GLB privacy statute. Consumer privacy would retain broad protections, without the additional costs of compliance with duplicative regulation.

To support this key recommendation, we have attached detailed comments describing certain operational impacts and conflicts relative to BCBS Plans. We have also provided recommendations and alternatives that we hope will prove helpful as the regulations are finalized.

We look forward to working with the federal agencies in achieving a workable balance that truly maximizes benefits for consumers. Please call Christina Nyquist at (202) 626-4799 if you have any questions.

Sincerely,



Mary Nell Lehnhard

Enclosure
Detailed Comments

cc: Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation
Office of Thrift Supervision
Federal Trade Commission
Securities and Exchange Commission
National Credit Union Administration
Department of Health and Human Services
National Association of Insurance Commissioners

Detailed Comments: Table of Contents

1) Purpose and Scope.....	2
2) Conflict With Other Laws, Regulations.....	2
3) Preemption: Relation to State Laws.....	3
4) Effective Date; Transition Rule.....	5
5) Definitions.....	5
6) Initial and Annual Notices.....	7
a) Initial and Annual Notice Required	
b) Information to be Included in Initial and Annual Notices	
c) When Initial Notice is Required to a Customer	
7) Limitation on Disclosures to Nonaffiliated Third Parties.....	11
a) Conditions for Disclosure	
b) Isolated Transaction With Consumer	
8) Exception to Opt Out for Service Providers and Joint Marketing.....	12
9) Marketing: Limits on Sharing of Account Number Information.....	13

Note: In the detailed text, each section title is followed by the citation to the Proposed Rule, as well as the page location.

1. Purpose and Scope

§216.1, P.-105

Explanation of Issue: The scope of the proposed rule applies to entities for which the Board has primary supervisory authority. These include: State member banks, bank holding companies and certain of their nonbank subsidiaries or affiliates, State uninsured branches and agencies of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and Agreement corporations.

We understand that the recently promulgated GLB privacy rules do not directly apply to BCBS Plans. However, BCBSA is submitting comments because the federal GLB privacy rules will likely be used as a baseline or precedent for future privacy laws and regulations adopted by the States.

Recommendation: BCBSA supports the continued regulation of health insurers and similar plans by locally based State insurance commissioners and believe it is important that the GLB privacy statute and privacy rules recognize this. However, to assure appropriate precedent, we recommend that the final GLB privacy regulation deem health plans that are subject to the proposed HIPAA privacy regulation as in compliance with the GLB privacy statute and regulations. Furthermore, we reaffirm our belief that other federal banking agencies participating in this joint rulemaking effort have no authority over BCBS Plans and urge their final rules to reflect this as well.

2. Conflict With Other Laws, Regulations

§216.1, P. 105

Explanation of Issue: Along with state laws and regulations, BCBS Plans are already subject to various federal laws and regulations related to privacy, including the proposed rule on standards for privacy of individually identifiable health information (HIPAA privacy rules), the Federal Privacy Act, and other laws.

BCBSA is concerned about the overlapping, duplicative, and conflicting nature of the GLB and HIPAA proposed privacy rules. This will result in confusion and higher costs for consumers and health insurers. Moreover, such duplication and conflict appear to defeat the cost-saving goals of HIPAA's administrative simplification provisions.

For example, the GLB privacy rules include provisions related to: contract requirements with nonaffiliated third parties; the ability of consumers to opt out of certain disclosures; notice requirements; and marketing restrictions. The HIPAA proposed privacy rules also include contract requirements with business partners; an authorization requirement for certain disclosures; notice requirements; and

marketing restrictions. While there are similarities between the two sets of standards, there are conflicts as well.

BCBSA is concerned that forcing health insurers to comply with both the HIPAA and GLB privacy rules would add unnecessary confusion and costs for consumers and health insurers.

Recommendation: Again, BCBSA repeats the recommendation that health insurers subject to the HIPAA privacy rules be deemed to be in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of a health insurer must be initiated under the HIPAA privacy regulations.

BCBSA has expressed our concern with aspects of the proposed HIPAA privacy rules through written comment, and we are continuing to work with the Administration toward developing more practical privacy protection solutions.

3. Preemption: Relation to State Laws

§216.15, P. 132

Explanation of Issue: The GLB regulation does not include a preemption of all state laws. State laws that offer greater protection than the federal law are specifically saved from preemption.

We are concerned that the lack of a complete preemption over state laws creates a serious compliance problem for financial institutions. Many health insurers, for example, operate across state lines. This incomplete preemption will require insurers to determine, on a provision by provision basis, which parts of state law would be retained, and which would be replaced by federal law.

This is further complicated by the free flow of patients and information in today's health care industry. For instance, an individual may live in the District of Columbia, work in Virginia, and visit a physician located in Maryland. Health insurers dealing with this individual must evaluate the interplay of three state statutes with the federal law. In addition, health insurers also must factor in the interplay of other federal laws relating to privacy. Such a multi-level compliance effort unnecessarily increases administrative costs, which ultimately effect consumers through higher premiums.

The evaluation of the interplay between state and federal laws will be particularly confusing for consumers. Instead of facilitating an individual's understanding of privacy rights, this complex preemption process is sure to confound consumers. First, individuals will be hard pressed to determine which aspects of the state and federal privacy laws apply to them, so it will be impossible for them to determine if in fact, they have been wronged.

In addition, consumers will not know where to direct complaints if they do feel that their rights are violated – Maryland? Virginia? The District of Columbia? The Secretary of Health and Human Services? The Federal Trade Commission? It is likely that consumers will be bounced from one jurisdiction to the next until the consumer locates the one which has the law that has been violated – or the consumer becomes frustrated and terminates the effort.

Recommendation: Financial institutions will be unable to navigate the labyrinth of state privacy laws and federal law under the complex construct of federal privacy laws and regulations, such as GLB and HIPAA. However, we also recognize that a complete preemption of state law is outside the statutory authority of the federal agencies with jurisdiction over GLB.

Therefore, we recommend that the federal agencies responsible for regulating GLB, in collaboration with HHS, prepare a detailed privacy guide that would show financial institutions and other covered entities which laws they must comply with when operating in each state across the country. The guide should be prepared in collaboration with state government officials to develop a statute-by-statute guide to the intersection of state and federal law. The guide should also assure incorporation of other federal privacy laws and regulations, including the Federal Privacy Act, HIPAA's privacy of individually identifiable health information, and others.

Again, for purposes of this guide, health insurers should be deemed to be in compliance with the GLB privacy statute if such insurers are subject to the HIPAA privacy rules.

As part of this process, each individual state should certify agreement with the guide so that health insurers and other financial institutions are protected against prosecution by individual states.

It is imperative that this legal guidebook is prepared well in advance of the final regulations. Financial institutions will need this completed analysis before computer systems can be modified, forms and notices are changed, contracts are updated, and other procedures can be brought into compliance. Bringing institutional operations into compliance with these complex new regulations will be expensive, so it is critical that financial institutions only have to modify systems and other items once. Therefore, we recommend that the analysis be provided two years prior to the effective date of the regulation. We also recommend continuous updating of this preemption guide.

4. Effective Date; Transition Rule

§216.16, P. 132

Explanation of Issue: The effective date of the GLB regulations is November 13, 2000. Implementation must occur within six months of that date. Financial institutions must provide an initial notice to existing customers no later than 30 days after the effective date. Of course, the effective date for health insurers would depend on state actions. In contrast, the effective date of the HIPAA regulations remains unclear (although by all accounts the regulations will be in final form before the end of this Administration). BCBSA is concerned about the lack of clarity regarding the effective date for health insurers. In addition, BCBSA is concerned that the 30-day requirement for initial notices is insufficient.

Recommendation: Again, BCBSA recommends that the regulations clearly state that health insurers subject to the HIPAA privacy rules are deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations. We also recommend that the publication of HIPAA and GLB final privacy rules be coordinated with each other.

Regardless, it is also important to recognize that a six-month compliance period is inadequate. A minimum of two years would be necessary to make the myriad number of changes necessary to assure compliance. In addition, we recommend that the 30 day initial notice requirement be revised to give health insurers enough time to update and distribute notices as part of normal mailings – such as with the Summary Plan Benefit Description.

See other recommendations on the need for a two year compliance period under our comments under No. 3 above – Preemption: Relation to State Laws.

5. Definitions of “Nonpublic Personal Information,” “Personally Identifiable Financial Information,” and “Publicly Available Information”

§216.3(n), §216.3(o), §216.3(p), P. 112-114

Explanation of Issue: The definition of information subject to privacy regulations under GLB and HIPAA differ. Therefore, some information will fall under both regulations, while other insurance information will fall only under HIPAA. These differences will likely make it difficult for consumers to understand their rights and for insurers to administer them.

For example, the HIPAA privacy regulations cover “*protected health information*” (PHI), which is individually identifiable health information that is electronically transmitted or maintained by a covered entity. The GLB Act and regulations protect “*nonpublic personal information*” (NPI), which is defined as personally identifiable financial information (i) provided by a consumer to a

financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by a financial institution. Such information does not include “*publicly available information*” . . . [but does include] any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

The regulations proposed by the federal agencies for GLB, except for those proposed by the Board of the Federal Reserve System (the one used as a main reference for this comment letter), provide two alternative definitions of NPI. The distinction lies in what is considered “publicly available.” Under Alternative A, information is “publicly available” only if it is obtained from government records, widely distributed media, or government-mandated disclosures. Under Alternative B, information is “publicly available” only if it is available from a public source.

“*Personally identifiable financial information*” is not defined by the Act, but is defined in the regulations to mean “any information: (1) provided by a consumer to [a financial institution] to obtain a financial product or service [from the financial institution]; (2) about a consumer resulting from any transaction involving a financial product or service between the [the financial institution] and a consumer; or (3) [the financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer.”

First, BCBSA is concerned about the overlap between information that is NPI and information that is PHI under the HIPAA privacy rules. The result will be confusion and higher costs for consumers and health insurers. Such duplication conflicts with the cost-saving goals of HIPAA’s administrative simplification provisions. For example, it is unclear whether health insurance companies would have to obtain from consumers both HIPAA-required authorizations, as well as opt out directives required under the GLB for personal information that falls under both PHI and NPI.

Second, BCBSA believes Alternative B is the correct interpretation that is consistent with the spirit of GLB. We believe that information that is available from a public source is, by definition, not private information. To attempt to privatize this information would increase consumer costs, while not providing any additional benefit to consumers – since the information is ultimately public anyway.

Third, the definition of *personally identifiable financial information* does not include “personally identifiable” in any of its subparts, but rather “any

information.” It is important to clarify this to assure that an unnecessarily and unintended broad scope of information is not included.

Recommendation: BCBSA recommends that health insurers subject to the HIPAA privacy rules are deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations.

Regardless, BCBSA recommends the following:

- Adopt Alternative B for the definition of NPI.
- Clarify the interaction of GLB protections for NPI and HIPAA’s privacy protections for PHI.
- Revise the definition of “personally identifiable financial information” by adding the words “personally identifiable” after the word “any” on line 1 of page 113 of the NPRM promulgated by the Federal Reserve Board. Also add “personally identifiable” before the word “information” in the examples listed under §216.3(o)(2) on page 113.

6. Initial and Annual Notices

a) Initial Notice and Annual Notice Required

§216.4, P. 115, §216.5, P. 119

Explanation of Issue: Under GLB, entities must provide:

- an initial notice to consumers of privacy policies and practices, as well as
- an annual notice to customers.

First, BCBSA is concerned that the notice requirements will confuse, rather than assure individuals about their privacy protections. Many individuals conduct financially related transactions with a number of different financial institutions. As a result, individuals would receive multiple notices from different entities under the proposed notice requirements.

Second, the notice requirements conflict with the notice requirements under HIPAA’s proposed rule on privacy of individually identifiable health information, which requires covered entities to provide notices to covered individuals:

- At enrollment;
- When material changes are made to privacy policies and procedures;
- No less frequently than every three years; and,
- Upon request.

Finally, clarification is needed that financial institutions can include notices as part of their routine mailings or electronic postings. Requiring separate mailings of notices would add unnecessary costs.

Recommendation: BCBSA recommends that health insurers subject to the HIPAA privacy rules are deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations. At a minimum, since health insurers are already subject to HIPAA’s privacy rule notice requirements, BCBSA feels that health insurance companies should be exempt from the GLB notice requirements.

Regardless, BCBSA recommends revision of the initial and annual notice standards so that they are more consistent with HIPAA’s notice requirements when final rules are issued. In addition, we recommend revisions for financial institutions as follows:

- Financial institutions should be allowed to include notices as part of materials that are regularly distributed (e.g., Summary Plan Benefit Description, for health insurers), or posted as part of their website. This would assure individuals receive the notices without unnecessary administrative expenses.
- The GLB and HIPAA privacy notices should be allowed to be combined.
- Only one notice per family be required for compliance. This would apply to the initial notice, annual notice, and subsequent notices.
- Delete annual or other subsequent notices and revise to state that subsequent notices (after the initial notice) are only required upon request by an individual or when material changes are made to privacy policies and procedures.

b) Information to be Included in Initial and Annual Notices
§216.6, P. 119

Explanation of Issue: This provision specifies the types of information that must be included in initial and annual notices of privacy policies and practices. For example, the notices must include categories of nonpublic personal information that the financial institution collects and discloses, categories of affiliates and nonaffiliated third parties to whom information is disclosed, explanation of the consumer opt out, and the institution’s policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.

First, as discussed above, BCBSA is concerned that the notice requirements will confuse, rather than assure individuals about their privacy protections. Many individuals conduct financially related transactions with a number of different financial institutions. As a result, individuals would receive multiple, possibly conflicting notices from different entities under the proposed notice requirements.

Second, the information required in notices is similar, but differs somewhat from the information required in notices under HIPAA's proposed rule on privacy of individually identifiable health information. This will lead to further confusion if the states enact their own financial and health privacy laws requiring even more notices, with even more information. As a result, it appears that health insurance companies could have to send at least two separate privacy notices to policyholders, leading to higher costs and confusion for consumers.

Third, subsection (c) of this provision regarding "future disclosures" is impractical. The fast-changing, innovative nature of financial and insurance businesses would make it impossible for an entity to predict its future disclosures accurately.

Fourth, while subsection (d)(4) of this provision allows for simplified notices in limited cases, we are concerned that the detail required in the notices could affect the efficiency and timeliness of certain isolated transactions for consumers and customers. Moreover, subsection (d)(2) of this provision states that "you do not adequately categorize the information that you disclose if you use only general terms." As a result, requiring detailed notices for isolated transactions could delay coverage decisions for our subscribers. For example, an isolated transaction for an insurer may include when an individual calls customer service. Clarification is needed to ensure that simplified notices are allowable for all isolated transactions.

Finally, subsection (d)(5) states that the financial institution must describe its policies and procedures with respect to protecting the confidentiality and security of nonpublic personal information by explaining "who" has access to the information and the circumstances under which the information may be accessed. This is inconsistent with the other subsections which refer to "categories" of information, as opposed to specific individuals. Revision is needed to make subsection (d)(5) consistent with the other subsections. Otherwise, the financial institution would have to detail the name of every employee or other individual having access to information, rather than the categories of personnel.

Recommendation: Since health insurers are already subject to HIPAA's privacy rule notice requirements, BCBSA feels that health insurance companies subject to the HIPAA privacy rules should be deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations.

Regardless, BCBSA recommends revision of the notice standards:

- Information required in GLB notices should be consistent with information required in notices under HIPAA's privacy rules for individually identifiable health information.
- Delete §216.6(c) regarding "future disclosures."
- Clarify §216.6(d)(4) so that simplified notices are allowed for all isolated transactions.
- Revise §216.6(d)(5) by deleting the words "who has access" and replacing with the words "the categories of personnel who have access"

c) When Initial Notice is Required to a Customer

§216.4(a)(1), P. 115

Explanation of Issue: In general, financial institutions must provide an initial privacy notice to an individual who becomes its customer, prior to the time that a customer relationship is established.

BCBSA is concerned that it would be difficult to know in advance whether a customer relationship would be established or not, when initially interacting with a consumer. This is another example of why flexibility in the provision of notices is important. Financial institutions should be able to include notices as part of application materials, post notices to web sites, and use other distribution mechanisms consistent with the normal course of interactions with consumers.

Otherwise, without knowing in advance whether a customer relationship would be established or not, this provision could be interpreted to require the financial institution to follow the rigid initial notice rules for any consumer with whom the organization interacts.

Recommendation: BCBSA recommends that health insurers subject to the HIPAA privacy rules are deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations. At a minimum, since health insurers are already subject to HIPAA's privacy rule notice requirements, BCBSA feels that health insurance companies should be exempt from the GLB notice requirements.

Regardless, we recommend that financial institutions should be allowed to include initial notices on web sites, as part of the regular mailings, and other publicly available sources.

7. Limitation on Disclosure of Nonpublic Personal Information About Consumers to Nonaffiliated Third Parties

a) Conditions for Disclosure

§216.7(a)(1), P. 122

Explanation of Issue: Subject to certain exceptions under §216.10 and §216.11, the GLB regulations prohibit financial institutions from disclosing NPI directly or indirectly to nonaffiliated third parties unless the financial institution has: (1) provided the consumer with an initial notice; (2) provided the consumer with an opt out notice; (3) given the consumer reasonable opportunity to opt out of the disclosure; and (4) the consumer has chosen not to opt out. In contrast, the HIPAA proposed privacy rules include requirements for health insurers to obtain authorizations from individuals for the use or disclosure of PHI under certain situations, but not for treatment, payment, health care operations, and other exceptions (e.g., public health, law enforcement, etc.).

The GLB opt out is similar to the HIPAA authorization requirement in some ways. For example, like the HIPAA authorization, there are various exceptions to the GLB opt out, including processing and servicing transactions, account administration, processing insurance claims, and administering insurance benefits. In addition, no opt out is required for disclosures to affiliates.

BCBSA is concerned, however, that there are significant administrative issues and conflicts between GLB and HIPAA. For instance, it is unclear whether a health insurer would be required to obtain both an authorization and an opt out from a consumer in situations involving the same personal information and use or disclosure.

Recommendation: BCBSA recommends that health insurers subject to the HIPAA privacy rules should be deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations. Such a deeming would clarify that health insurers would not be required to obtain both an authorization (as required under the HIPAA privacy rules) and an opt out from a consumer (as required under GLB).

b) Isolated Transaction With Consumer

§216.7(a)(3)(ii), P. 123

Explanation of Issue: This provision requires opt out notices to be given at the time of isolated transactions with a request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction. BCBSA is concerned that the detail required in the notices could

delay coverage decisions for our subscribers. For example, an isolated transaction may include the situation where an individual calls customer service or submits a request via fax or Internet that would require us to make a disclosure to complete the transaction. Clarification is needed to ensure that simplified notices are allowable for all isolated transactions.

Recommendation: Health insurers subject to the HIPAA privacy rules should be deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations. Regardless, we recommend that simplified opt out notices are allowable for all isolated transactions.

8. Exceptions to Opt Out Requirements for Service Providers and Joint Marketing §216.9, P. 126

Explanation of Issue: Subject to further exceptions under §216.10 and §216.11, this provision allows for an exception to the opt out requirements when a financial institution discloses NPI about a consumer to a nonaffiliated third party to perform services for or on behalf of the financial institution, if the financial institution: (1) provides the initial notice; and (2) enters into a contractual agreement with the third party that: (i) requires the third party to maintain the confidentiality of the information; and (ii) limits the third party's use of information solely to the purposes for which the information is disclosed or otherwise permitted by §216.10 and §216.11. This provision specifically includes joint marketing efforts.

First, although there are exceptions to this provision, BCBSA is concerned that this provision potentially could expose health insurers to more liability, forcing them to monitor nonaffiliated third parties under certain circumstances. Moreover, it is unclear how this provision interacts with the business partner and chain of trust agreements under the HIPAA proposed rule on privacy of individually identifiable health information and Security and Electronic Signature Standards NPRM.

Second, we are concerned that this provision could disrupt existing contractual arrangements between BCBS Plans and nonaffiliated third parties. Simultaneously renegotiating such a large volume of contracts could lead to unnecessary cost increases in the price of services for consumers.

Recommendation: Once again, we believe health insurers, since they are covered by the HIPAA privacy rules, should be deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations. These GLB provisions overlap and conflict with the HIPAA privacy rule business partner and chain of trust standards. Regardless of the overlapping problems,

BCBSA has serious concerns with the GLB contract requirements as currently drafted.

We recommend clarification that:

- No financial institution would be subject to penalties or liability for breaches of privacy made by a nonaffiliated third party.
- No financial institution would be subject to penalties or liability for failure to monitor nonaffiliated third parties or any other organization.
- Contract changes would only be required upon contract renewals or issuance; current contracts would not have to be re-opened immediately.

We believe these standards could be addressed by requiring nonaffiliated third parties to certify compliance with the NPRM on privacy of consumer financial information. Such certification would include hold harmless and indemnification clauses to remove responsibility from any other financial institution or other entity.

9. Marketing: Limits on Sharing of Account Number Information for Marketing Purposes

§216.13, P. 131

Explanation of Issue: Entities may not disclose an account number or similar form of access number or access code for a credit card account, deposit account or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

BCBSA is concerned about the vagueness of certain terms in this section. We do not believe it is the intent, nor is it our interpretation, that health insurance subscriber identification numbers would fall under “account number” or “access number” or “transaction account.” Without clarification, however, since “marketing” is also not defined, this provision could have the unintended consequence of deterring health insurers from contracting out important customer service or health improvement activities via direct mail, electronic mail, or similar means.

Health plans frequently engage in activities for improving their subscribers’ treatment and quality of care – such as disease management programs, mammography reminders, sending newsletters with new research articles to members, promotions for treadmills or exercise club memberships, providing provider lists to members, wellness programs, drug formularies, drug rebate

programs, etc. Many of these activities involve some form of mailing to subscribers.

Consumers also benefit when they learn about new products and services from their health plan. Other examples of activities conducted include:

- Many Blues Plans notify older subscribers that they qualify for Medicare and no longer need their current comprehensive policy, but that we offer Medigap products that could provide additional benefits.
- When subscribers move out of a Plan service area, some BCBS Plans provide subscribers with information regarding special programs – such as guaranteed issue products – offered by their new local Blue Plan.
- BCBS Plans direct subscribers to beneficial products – for instance, notification to subscribers regarding potential eligibility for CHIP, or Special CARE (a private program for low-income enrollees), or Caring Foundation bridge programs or other products that could benefit specific elements of the population.
- Individuals and small employers enjoy convenient “one-stop shopping” with health plans that also offer property and casualty and life insurance products.

Recommendation: BCBSA recommends that health insurers subject to the HIPAA privacy rules are deemed in compliance with the GLB privacy statute – meaning that any action or investigation of the practices of that health insurer must be initiated under the HIPAA privacy regulations.

Regardless, BCBSA recommends:

- Clarifying that health insurance subscriber identification numbers do not fall under this provision.
- Clarifying the definition of “marketing” so that beneficial programs such as the ones described above may continue.