HIPAA Privacy

For our Group Customers and Business Partners

Independence Blue Cross

HIPAA, The Health Insurance Portability and Accountability Act of 1996, established rights and protections for health care consumers and created responsibilities for health Plan Sponsors. In the initial phase, HIPAA provided guidelines to insurers and their customers for minimum standards of health coverage, the administration of pre-existing conditions and guaranteed renewal for health insurance products.

HIPAA Title II, also referred to as Administrative Simplification, creates standards that relate to both the simplification of communication among parties in using electronic transactions and to the privacy and security of member-specific information.

This brochure focuses on the HIPAA Privacy Rule and is developed as an information piece for our group customers and their business partners to assist you in identifying potential areas for review and action. The full text of the Privacy Rule can be found at **http://hhs.gov/ocr/hipaa/finalreg.html**

HIPAA Privacy Rule—Introduction

The HIPAA Privacy Rule, which went into effect on April 14, 2001, will require compliance on April 14, 2003. This Rule offers the first comprehensive federal protection for the privacy of individuals' health information. The U.S. Department of Health and Human Services Office of Civil Rights will enforce the Rule.

The Privacy Rule governs the use and disclosure of Protected Health Information ("PHI"), which is individually identifiable health information. The federal Privacy Rule is considered a "floor" of Privacy standards and may be superceded by more stringent state privacy and confidentiality laws and regulations. Employer sponsored health plans, and in some situations the plan sponsors that provide certain services in connection with their health plans, will face compliance requirements from this Rule.

This document should be considered as informational only and is not meant to convey legal advice or counsel. IBC's group customers and business partners should involve their legal counsel to advise and assist them in determining what they must do to meet their specific obligations under the HIPAA Privacy Rule.

Table of Contents

Section 1: Overview of HIPAA Title II—Administrative Simplification

Administrative Simplification is the official name of Title II Subtitle F of the Health Insurance Portability and Accountability Act of 1996. This provision of the Act defines terms and requirements for:

- Electronic Data Standardization
- Security; and
- Privacy

Electronic Data Standardization

Today, many providers and health insurance companies exchange information electronically in hundreds of different formats. Electronic Data Standardization requires that all Covered Entities use standard formats and standard codes for electronic transactions effective October 16, 2002 or, if they filed for an extension with the Department of Health and Human Services, effective October 16, 2003.

Security

The proposed security rules, which at this time have not been finalized and do not have a specific date for compliance, will require implementing security standards to protect and ensure the privacy and confidentiality of individually identifiable health care information.

Privacy

The Privacy Rule, which will require compliance by April 14, 2003, is designed to restrict the use and disclosure of health related information to appropriate purposes and to ensure that employee health information is not used against individuals in connection with their employment.

Who Must Comply

Organizations that are directly affected by the HIPAA regulation are referred to under the law as **covered entities**. These include:

- Health plans (including health insurers, HMOs, managed care plans, and group health plans sponsored by Employers, Health and Welfare Funds, and Associations;
- Healthcare clearinghouses who convert nonstandard formats to compliant transactions; and,
- Healthcare providers who transmit health information in electronic form.

These HIPAA regulations have a number of implications not only for group customers' health Plan Sponsors, but also for their agents and brokers, even though they are not "covered entities".

Section 2: The Privacy Rule—Key Definitions

The following are some key terms. We urge you to become familiar with them because they will help you understand and meet the compliance requirements associated with the rule.

Protected Health Information (PHI): Individually identifiable health information, transmitted or maintained in any form or medium (including electronic media), including demographic information collected from an individual, that relates to:

- The provision of health care to an individual; or
- The past, present or future physical or mental health or condition of an individual or payment for the provision of health care to an individual; and
- The information identifies the individual or there is a reasonable basis to believe that the information can be used to identify the individual.

Summary Health Information: Summary health information is information that may be individually identifiable information, and that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor (the employer, health and welfare fund or association that "sponsors" the health benefits plan) has provided health benefits under a group health plan and from which most identifiers have been removed.

Minimum Necessary: Covered entities generally are required to use, disclose and request only the minimum necessary PHI to accomplish the purpose of the request. This concept is called "minimum necessary" under the Privacy Rule.

Business Associate: an external nonaffiliated third party, individual or entity that provides services or assistance to a covered entity related to treatment, payment for treatment, or healthcare operations. Indirectly, business associates of covered entities are subject to the Privacy Rule because of contractual requirements that are mandated.

ERISA Plan: An employee welfare benefit plan of the Employee Retirement Income and Security Act of 1974 (ERISA) 29 U.S.C. § 1101 et seq.

Health Plan: An individual or group plan that provides, or pays the costs of medical care. A health plan includes group health plans, health and welfare funds, health insurers, HMOs, managed care plans, essentially all government health plans such as FEHB, and public health programs such as Medicare, Medicare supplemental plans, and Medicaid.

Group Health Plan: The component of the Employer, Health and Welfare Fund or Association (group customer) who may require access to other members' PHI to perform their day-to-day job functions of administering the overall health benefit plan and health benefits for members of the group customer. These individuals usually work within the human resources/employee benefits area of the group customer.

Plan Sponsor: Generally an entity that offers the group health plan to its members (as defined by the ERISA statute). Representatives of a plan sponsor may be a director, senior executive, or all other employees who do not require access to members' PHI to perform their day-to-day job functions. With minor limitations for enrollment information and Summary Health Information for certain purposes, access to the members' PHI by the plan sponsor requires an amendment to the Plan documents and other Privacy Rule compliance obligations.

The Privacy Rule—Objectives and Requirements

The Privacy Rule:

- Gives patients more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that health care providers, health plans and others must achieve to protect the privacy of health information.
- Holds violators accountable, with civil and criminal penalties that can be imposed if they violate an individual's privacy rights.
- And strikes a balance when public responsibility supports disclosure of some forms of data—for example to protect public health.

The Privacy Rule uses the structure created by ERISA, which sets up two distinct components within an entity offering health insurance benefits to employees to set its requirements. These components are the plan sponsor (i.e., the Employer, Health and Welfare Fund or Association) and the group health plan (i.e., the benefit plan itself, represented by those who administer the plan).

The Privacy Rule creates a regulatory barrier to restrict the flow of PHI between a group health plan and the plan sponsor. The primary goal of this separation is to prevent the group customers from using their employees' or members' PHI when making employment-related decisions.

The Privacy Rule sets requirements for:

- Establishing policies and procedures, including handling complaints, appointing a privacy officer, record retention, and providing staff training
- Providing a "Notice of Privacy Practices"
- Contracting with "Business Associates"
- Using and disclosing PHI
- Establishing appropriate administrative, technical, and physical safeguards
- Acting promptly to correct a violation or otherwise lessen the harmful effects of a violation
- Providing a process for individuals to exercise their rights to access their PHI, amend their PHI, and to restrict the use of their PHI

Section 3: Specific Requirements for our Group Customers and Business Partners

Of the three components of Administrative Simplification, the Privacy Rule will have the most impact on our group customers and their business partners. The following section outlines the impact of this rule.

While the HIPAA Privacy Rule does impose new obligations on the entire health care industry, this Rule does not affect the benefit design of the programs offered by our customers, the services provided under these programs, the provider networks available to their members or the day-to-day operations of providing health care benefits.

Group Health Plans and their Plan Sponsors must follow special rules in connection with the Privacy Rule. The Privacy Rule does not directly regulate plan sponsors; it does, however, regulate the group health plans sponsored by these plan sponsors. Where PHI is shared with the Plan Sponsor, the Rule also imposes obligations on the Plan Sponsor. Therefore, the Privacy Rule will have a direct effect on the health plans of our group customers and in some circumstances, additional effects on sponsoring entities as well.

Impact for Fully-Insured Group Health Plans

A group health plan is subject to limited HIPAA obligations if, and only if, it meets two criteria:

- The plan provides benefits solely through an insurance contract with an insurer or HMO (i.e., is fully insured); AND
- The plan does not create or receive PHI. (The plan may receive summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO.)

The limited obligations include:

- Refrain from interfering with employees exercising their rights under the Privacy Rule (e.g., requesting access to or a copy of their health information, filing a privacy complaint); and,
- Refrain from requiring any person to waive rights under the Privacy Rule as a condition of receiving payment, enrolling in a health plan or being eligible for benefits.

Impact for Fully-Insured Group Health Plans that do not Receive PHI

The fully-insured group health plan that does not receive PHI can continue to do the following:

- Perform enrollment functions;
- Receive summary health information for any treatment, payment, or operation purposes;
- Act as an advocate for the member in claim processing issues but may be required to obtain the individual's authorization if they wish to avoid additional HIPAA compliance obligations.

Impact for Fully-Insured Group Health Plans that Receive PHI, Self Insured Plans/ Cost Plus Plans

Generally, group health plans that fall into this category must fully comply with the Privacy Rule in the same way that a health insurer or provider would have to comply. In addition to the "limited obligations" (above), fully insured group health plans that receive PHI and self-insured and cost-plus group health plans must:

- Appoint a privacy official that is responsible for the development and implementation of the health plan's policies and procedures;
- Designate a contact person (or office) who is responsible for receiving complaints filed under the Privacy Rule;
- Establish policies and procedures concerning PHI that comply with the Privacy Rule;
- Train all members of the workforce on health plan's PHI policies and procedures;
- Establish appropriate administrative, technical and physical safeguards to protect the privacy of PHI from intentional or unintentional use or disclosure that violates the Privacy Rule;
- Provide a process for individuals to make complaints concerning the group health plan's policies and procedures, or its compliance with its policies and procedures for the Privacy Rule;
- Establish and apply appropriate disciplinary measures against members of its workforce for violations of the group health plan's policies and procedures, or the Privacy Rule;
- Act promptly to correct a violation or otherwise lessen the harmful effects resulting from a violation of its policies and procedures about which it has knowledge;
- Prepare and distribute a Notice of Privacy Practices to all individuals in the health plan;

- .Provide the individual the right to request access, amendment, accounting, confidential communications and restrictions of PHI; and
- Retain compliance documentation for six years.

Impact for Plan Sponsors

A plan sponsor's obligations will vary depending on receipt of:

- no health information at all
- summary health information or
- PHI

If the plan sponsor does not receive any health information at all (neither PHI nor summary health information), the plan sponsor has no formal compliance obligations under HIPAA Title II.

If the plan sponsor does not receive PHI, but only receives summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO, the impact of the Privacy Rule will be minimal. Summary health information may be released to a plan sponsor if the plan sponsor agrees to only use the information to obtain premium bids for providing health insurance coverage to the group health plan; or modify, amend or terminate the group health plan.

If a plan sponsor receives PHI in order to manage its health benefits program, the compliance requirements increase dramatically. Before the plan sponsor may receive PHI from either the group health plan or the insurer, it must "certify" to the group health plan that its plan documents have been amended to incorporate the following provisions, and that it agrees to abide by them as follows:

- Only disclose PHI as permitted by the plan documents or as required by law;
- Not use or disclose the PHI for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the sponsor;
- Ensure that "adequate separation" of records and employees is established and maintained between the group health plan and the plan sponsor;
- Ensure (through a written contract) that the plan sponsor's agents and subcontractors (e.g., benefits consultants) agree to abide by the same restrictions and conditions as the plan sponsor in regard to the use of PHI received from the group health plan;
- Report any improper use or disclosure of PHI to the group health plan;
- Allow individuals to inspect and obtain copies of PHI about themselves;

- Allow individuals to request to amend PHI about themselves;
- Provide individuals with an accounting of disclosures of PHI made within the six years prior to the request for such accounting; and
- Make its internal practices, books and records relating to the use and disclosure of PHI available to the Department of Health and Human Services (HHS) for purposes of auditing the group health plan's compliance with the Privacy Rule.

NOTE: **Regardless of which of the above categories the group customer falls into, you should take special care to protect any member health information to ensure that this information is used only for appropriate purposes.**

Section 4: Group Health Plans and their Business Associates

When group health plans have taken the necessary steps to become HIPAA compliant based on their fully-insured or self-insured status as well as the amount of PHI they elect to receive or create, they must take steps to require their business associates to be HIPAA-compliant as well. A business associate is an external nonaffiliated third party that the covered entity contracts with to perform a covered function(s) on its behalf involving the use or disclosure of PHI. For example, an insurer that provides third party administration for a self-insured plan is the business associate of the self-insured plan.

Group health plans that share PHI with their business associates must obtain "satisfactory assurance" that their business associate will safeguard their enrollees' PHI. This is accomplished by executing a written contract or contract amendment with its business associates, which contractually obligates the business associate to protect the PHI that they create, receive, use or disclose. Therefore, the business associate contracts must specify that the business associate:

- Must use and disclose PHI only as permitted by the contract with the group health plan and consistent with the Privacy Rule;
- Must implement data privacy and security safeguards;
- Must ensure any agents or subcontractors they employ to assist in fulfilling their contract obligations to the group health plan adhere to the same restrictions;
- Must provide enrollees with access, amendment and disclosure accounting upon request;

- Must report improper use or disclosure of PHI to the group health plan
- Must make its books and records available to the Department of Health and Human Services (DHHS) upon request;
- Must return or destroy PHI at the end of the contract if feasible to do so. If not feasible, the business associate must ensure that no improper use or disclosure of PHI occurs.

Section 5: Your Relationship with IBC under HIPAA

IBC has spent significant time examining how the HIPAA Title II regulations affect our business relationship with our group customers and business partners. We believe the policies IBC has developed to ensure compliance will allow both IBC and our group customers and their business partners to continue to provide health care benefits with minimal disruption to the service you and your members enjoy from IBC.

The following outlines the procedures we will follow in responding to specific requests from our group customers for PHI regarding an individual member, as part of the Plan's efforts to provide assistance to individual employees or members. Under HIPAA, IBC will only provide Protected Health Information (PHI) on an individual member to a group health plan as follows:

- We will inform the group health plan representative that we will take his/her question or issue, but will return the call directly to the member; or
- If the member is in the presence of the group health plan representative while he/she is attempting to contact us, we will accept a verbal authorization from the member, note that in our records, then discuss the issue with the health plan representative and member; or
- If the first and second options listed above are not possible, we will ask the group health plan representative to fax us an authorization completed by the member that will allow us to disclose PHI to the person designated on the authorization form.

Section 6: What you should be doing now

Before deciding the path your company will take to become compliant, you must first understand and analyze the HIPAA Title II Privacy Rule as it applies to your health benefit plan(s). By answering the following questions, you can begin to plan your strategy:

Self-Check

- Is the plan fully insured, or self-insured/cost-plus?
- Does the group customer rely on an insurer to handle day-to-day operations of the plan? Or does the group customer use a traditional third-party administrator?
- How involved is the group customer in the operation of the plan?
- What kinds of information does the group customer receive about members enrolled in its group health plan?

Next, assess whether your company plan sponsor or group health plan requires PHI by answering the following:

Plan Sponsor

- Does the group customer, as Plan Sponsor, wish to be involved in the overall management of the group health plan?
- If so, can the Plan Sponsor accomplish its business goals by performing the plan administration functions without receiving any PHI?
- If the Plan Sponsor feels that it must receive or use PHI to achieve its goals, then the Plan Sponsor will need to comply with the HIPAA Privacy requirements outlined in this booklet in order to receive PHI either from the group health plan directly or from an insurer or other entity involved in administering the plan.

Group Health Plan

- Is the plan fully insured or self-insured/cost-plus?
- If fully insured, does the group health plan need to receive PHI to administer the health plan?
- If the plan is fully insured and does not receive PHI, other than enrollment or summary health information, then the plan may be able to avoid many of the compliance obligations imposed by HIPAA. If the fully insured plan does receive PHI, it will need to comply with the full range of requirements imposed by HIPAA.
- If self-insured or cost-plus, how will the plan meet all of the HIPAA compliance obligations?

Section 7: Other "Things to Know"

Notice of Privacy Practices

IBC will be publishing the Notice of Privacy Practices as an insert in the UPDATE magazine that is mailed to all subscribers. The mailing will begin at the end of February 2003 and will be completed by the end of the first quarter. Additionally, the Notice of Privacy Practices will be included in new member enrollment packets. A copy of IBC's Notice of Privacy Practices is included in this mailing and will be published on the ibx.com web-site as required by the Privacy Rule.

Individual Rights

The Privacy Rule provides an individual with rights to:

- access their protected health information,
- amend their protected health information,
- request an accounting of disclosures of their protected health information,
- request confidential communications,
- request restrictions to the use or disclosure of their protected health information.

IBC will handle all requests for "Member Rights"—Access, Amendment, Accounting, Confidential Communication and Restrictions of PHI **BUT** IBC will notify the member that IBC may not have all of the information and the member should contact their group health plan.

IBC may impose a reasonable fee on the individual for access requests and for more than one accounting request within 12 months. IBC will allow the individual to modify the request to avoid any applicable fees.

Authorizations for Disclosure

As stated in this booklet, individual authorizations must be obtained prior to the release of PHI for the purpose of resolving member concerns or for certain purposes permitted by the Privacy Rule. Generally, an individual authorization is voluntary and must be completed by the individual in clear and understandable language prior to any disclosure. IBC will make an authorization form available to you to use with your employees/members. IBC reserves the right to request an authorization before any disclosure including those for treatment, payment and health care operations.

A sample authorization is included in this mailing. Additional copies are available on the ibx.com web-site or via your marketing representative.

Accountability and Enforcement

Covered entities that violate the Privacy Rule requirements are subject to penalties under HIPAA as indicated below. Enforcement will be through the Department of Health and Human Services Office of Civil Rights.

- Civil penalties are $100 per incident, up to $25,000 per violation per year per standard.
- Federal criminal penalties exist for covered entities that knowingly and improperly disclose information or obtain information under false pretenses. Criminal penalties include fines up to $50,000 and one year in prison for improperly obtaining or disclosing PHI; up to $100,000 and up to five years in prison for obtaining PHI under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.
- There is no statutory authority for a private right of action for individuals to enforce their Privacy Rights.

Other Permitted Disclosures

The Privacy Rule permits certain disclosures of PHI without individual authorization for certain national priority activities and for activities that allow the health care system to operate more smoothly. These activities include:

- Oversight of the health care system, including quality assurance activities;
- Public Health, reporting of disease and vital statistics;
- Research, generally limited to when a waiver of authorization is independently approved by a Privacy board or Institutional Review Board;
- Judicial and administrative proceedings;
- Limited law enforcement activities;
- Emergency circumstances;
- Identification of a deceased person or to determine the cause of death;
- Inclusion in facility patient directories;
- Activities related to national defense and security.

Section 8: Frequently Asked Questions

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It established rights and protections for health care consumers and created responsibilities for health insurers such as IBC and Keystone Health Plan East, health Plan Sponsors and their group health plans.

What is Administrative Simplification?

HIPAA Title II, also referred to as Administrative Simplification, creates standards that relate to both the simplification of communication among parties in using electronic transactions and to the privacy and security of member-specific information.

What is the Privacy Rule?

The Privacy Rule, a subset of Title II Administrative Simplification, governs the use and disclosure of Protected Health Information ("PHI").

How is "PHI" defined?

PHI is individually identifiable health information, transmitted or maintained in any form or medium (including electronic media). It includes demographic information collected from an individual that relates to the past, present or future physical or mental health condition of an individual or the provision or payment of health care. Essentially, for group health plans and health insurers, this means any individually identifiable information about health plan members.

This phrase (and the Privacy Rule itself) does not usually apply to health care information held by employers about their employees that is obtained in connection with employer functions outside of the operation of a health plan—such as employment applications, disability management and worker's compensation.

Is HIPAA the only Privacy Law?

HIPAA is a federal privacy law that sets a minimum national privacy standard. State(s) may enact privacy laws that provide greater privacy protections than HIPAA. Other federal laws also may be relevant in some situations.

Are there penalties for not complying with the HIPAA requirements?

Yes. There are both civil fines and criminal penalties, including imprisonment. The civil fines are $100 per violation, up to $25,000 a year for each standard violated. Criminal penalties for knowing misuse of protected health information may be as high as $50,000 and one year of imprisonment. There are higher criminal penalties for false pretenses and for intent to sell information.

What HIPAA Means to Me

Who is affected by the HIPAA Privacy Rule?

The HIPAA law requires covered entities to comply with the Privacy Rule. Covered entities include Health Plans (including health insurers, HMOs, managed care plans, and group health plans sponsored by Employers, Health and Welfare Funds, and Associations); health care clearing houses; and healthcare providers.

Is the Plan Sponsor of the Group Health Plan the covered entity?

Employers, health and welfare funds and associations ("group customers") that sponsor group health plans are not "covered entities" under HIPAA. The covered entity is the group health plan and not the employer itself. The group health plan is treated as a component within the group customer that provides medical benefits directly or through insurance.

Do group customers need to worry about complying with HIPAA? What if I'm a small group customer?

Almost every group customer that offers health benefits to its members will feel some effect from the HIPAA Privacy Rule. The extent of these obligations will depend on the financing structure of the health plan and the type of PHI received by the health plan, as well as whether the plan sponsor also receives PHI from the health plan. There is no exception for small employers, although in some situations small employers may have certain additional time to comply with the Rule.

What are my organization's obligations under HIPAA?

Group Health Plans and their Plan Sponsors must follow special rules in connection with the Privacy Rule. The Group Health Plan is a "covered entity" that must meet at least some HIPAA Privacy Rule obligations in all instances. Where PHI is shared with the Plan Sponsor, the Rule also imposes separate significant compliance obligations on the Plan Sponsor. Therefore, the Privacy Rule will have a direct effect on the health plans of our group customers and in some circumstances, additional effects on sponsoring entities as well.

Can a group health plan limit its obligations under HIPAA?

A group health is subject to limited HIPAA compliance obligations if, and only if, it meets these criteria:

1. The plan is fully-insured AND
2. The plan does not create or receive protected health information. All other Group Health Plans (meaning any self-insured group health plan or a fully insured plan that receives PHI) must comply with all requirements of the Privacy Rule.

An insured group health plan can continue to limit its HIPAA compliance obligations if it only receives summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO.

What are the limited obligations?

Every group customer must have a policy to refrain from interfering with employees exercising their rights under the Privacy Rule, e.g., requesting access to or a copy of their health information, filing a privacy complaint, etc. and to refrain from requiring any person to waive rights under the Privacy Rule as a condition of receiving payment, enrolling in a health plan or being eligible for benefits.

What happens if the Plan Sponsor receives PHI?

Before the plan sponsor may receive PHI from either the group health plan or the insurer, it must "certify" to the group health plan that its plan documents have been amended to incorporate the required HIPAA provisions, and, that it agrees to abide by them. These required provisions track many of the requirements imposed on group health plans and insurers, and create some specific additional obligations for plan sponsors (including the requirement that the plan sponsor/employer not use PHI in connection with employment-related decisions).

I heard that contracts with brokers and consultants need to be changed, is that true?

Under the HIPAA Privacy rule, if a Group Health Plan contracts with someone who will use or disclose PHI while performing services on your behalf, there are additional contract requirements. This contractor is called a "business associate" under the Privacy Rule. Specifically, the group health plan must enter into a Business Associate Agreement with each entity that provides services or assistance to a covered entity when such services or existence relate to treatment, payment for treatment or healthcare operations.

Do I need to change the way I handle medical information relating to pre-employment physicals, fitness-for-duty, drug-free workplace tests, etc.?

Plan Sponsors/employers generally can continue to engage in activities that involve employee medical information, as long as this information is not obtained from the group health plan. Accordingly, when an employer conducts pre-employment physicals, for example, the HIPAA Privacy Rule is not implicated.

In certain situations, a physician conducting these physicals may be a covered provider under HIPAA and therefore may require the employee to provide a HIPAA authorization before he or she will release the health information to the employer. However, once the employer receives the information, it becomes part of the employment file and is not considered PHI.

How does HIPAA affect medical information relating to workers' compensation cases?

HIPAA has a special rule permitting an employer to release information from its group health plan for purposes of complying with State and Federal workers' compensation laws. The disclosure must only include that information that is "authorized by" and "necessary to comply with" the relevant law. Information obtained outside of the health plan for workers compensation claims (for example, from the employee directly) is not subject to the Privacy Rule.

Your Relationship with IBC under HIPAA

Will I still be able to help my members resolve their claims issues?

Yes, you can continue to act as an advocate for the member in claims processing issues, but will have to obtain the member's authorization before IBC will discuss the issue with you. IBC has developed an authorization form for our members' use (a copy of which is included in this packet and which is also available on our website www.ibx.com).

Will IBC be providing a Privacy Notice to members enrolled in the group health plan?

IBC will include its Notice of Privacy Practices as an insert in the spring member newsletter(s) that are mailed to all subscribers. The Notice of Privacy Practices will then be included in new member enrollment packets. IBC will handle all requests for "Member Rights"—including Access, Amendment, Accounting, Confidential Communication and Restrictions of PHI BUT IBC will notify the member that IBC may not have all of the information and the member should contact their group health plan as well.

What You Should Be Doing Now

How do I get started?

Before deciding the path your company will take to become compliant, you should first understand the HIPAA Title II Privacy Rule as it applies to your health benefit plan(s). This will involve determining whether your company sponsors a group health plan, what kind of funding mechanism is in place for the group health plan and whether the group health plan receives, uses or discloses PHI in the operation of that Plan. You may wish to consult your legal counsel on these issues.

Where can I obtain a copy of the HIPAA regulations?

The Privacy regulations are available at www.hhs.gov/ocr/hipaa/finalreg.html. For information about the other final and proposed Administrative Simplification regulations, see aspe.hhs.gov/admnsimp/.

Section 9: Member Notice

Independence Blue Cross Notice of Privacy Practices*

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

Please review it carefully.

This Notice takes effect on April 14, 2003.

Independence Blue Cross values you as a customer, and protection of your privacy is very important to us. In conducting our business, we will create and maintain records that contain protected health information about you and the health care provided to you as a member of our health plans.

"Protected health information" or "PHI" is information about you, including information about where you live, that can reasonably be used to identify you and that relates to your past, present or future physical or mental health or condition, the provision of health care to you or the payment for that care.

We protect your privacy by:

- limiting who may see your PHI,
- limiting how we may use or disclose your PHI,
- informing you of our legal duties with respect to your PHI,
- explaining our privacy policies, and
- adhering to the policies currently in effect.

This Notice describes our privacy practices, which include how we may use, disclose, collect, handle, and protect our members' protected health information. We are required by certain federal and state laws to maintain the privacy of your protected health information. We also are required by the federal Health Insurance Portability and Accountability Act (or "HIPAA") Privacy Rule to give you this Notice about our privacy practices, our legal duties, and your rights concerning your protected health information.

This Notice takes effect on April 14, 2003, and will remain in effect until we replace or modify it.

*If you are enrolled in a self-insured group benefit program, this Notice is not applicable. If you are enrolled in such a program, you should contact your Group Benefit Manager for information about your group's privacy practices. If you are enrolled in the Federal Employee Service Benefit Plan, you will receive a separate notice.

Copies of this Notice

You may request a copy of our Notice at any time. If you want more information about our privacy practices, or have questions or concerns, please contact Member Services by calling the telephone number on the back of your Member Identification Card, or contact us using the contact information at the end of this Notice.

Changes to this Notice

The terms of this Notice apply to all records that are created or retained by us which contain your PHI. We reserve the right to revise or amend the terms of this Notice. A revised or amended Notice will be effective for all of the PHI that we already have about you, as well as for any PHI we may create or receive in the future. We are required by law to comply with whatever Privacy Notice is currently in effect. You will be notified of any material change to our Privacy Notice before the change becomes effective. When necessary, a revised Notice will be mailed to the address that we have on record for the contract holder of your member contract, and will also be posted on our web site at **www.ibx.com**.

Potential Impact of State Law

The HIPAA Privacy Rule generally does not "preempt" (or take precedence over) state privacy or other applicable laws that provide individuals greater privacy protections. As a result, to the extent state law applies, the privacy laws of a particular state, or other federal laws, rather than the HIPAA Privacy Rule, might impose a privacy standard under which we will be required to operate. For example, where such laws have been enacted, we will follow more stringent state privacy laws that relate to uses and disclosures of the protected health information concerning HIV or AIDS, mental health, substance abuse/chemical dependency, genetic testing, reproductive rights, etc.

How We May Use and Disclose Your Protected Health Information (PHI)

In order to administer our health benefit programs effectively, we will collect, use and disclose PHI for certain of our activities, including payment of covered services and health care operations.

The following categories describe the different ways in which we may use and disclose your PHI. Please note that every permitted use or disclosure of your PHI is not listed below. However, the different ways we will, or might, use or disclose your PHI do fall within one of the permitted categories described below.

Payment: We may use and disclose your PHI for all payment activities including, but not limited to, collecting premiums or to determine or fulfill our responsibility to provide health care coverage under our health plans. This may include coordinating benefits with other health care programs or insurance carriers, such as Medicare or Medicaid. For example, we may use and disclose your PHI to pay claims for services provided to you by doctors or hospitals which are covered by your health plan(s), or to determine if requested services are covered under your health plan. We may also use and disclose your PHI to conduct business with other IBC affiliate companies.

Health Care Operations: We may use and disclose your PHI to conduct and support our business and management activities as a health insurance issuer. For example, we may use and disclose your PHI to determine our premiums for your health plan, to conduct quality assessment and improvement activities, to conduct business planning activities, to conduct fraud detection programs, to conduct or arrange for medical review, or to engage in care coordination of health care services. We may also use and disclose your PHI to offer you one of our value added programs like smoking cessation or discounted health related services, or to provide you with information about one of our disease management programs or other available IBC health products or health services.

We may also use and disclose your PHI to provide you with reminders to obtain preventive health services, and to inform you of treatment alternatives and/or health related benefits and services that may be of interest to you.

Marketing: We may use your PHI to make a marketing communication to you that is in the form of (a) a face-to-face communication, or (b) a promotional gift of nominal value.

Release of Information to Plan Sponsors: Plan sponsors are employers or other organizations that sponsor a group health plan. We may disclose PHI to the plan sponsor of your group health plan as follows:

- We may disclose "summary health information" to your plan sponsor to use to obtain premium bids for providing health insurance coverage or to modify, amend or terminate its group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience for the individuals who participate in the plan sponsor's group health plan;
- We may disclose PHI to your plan sponsor to verify enrollment/disenrollment in your group health plan;
- We may disclose your PHI to the plan sponsor of your group health plan so that the plan sponsor can administer the group health plan; and
- If you are enrolled in a group health plan, your plan sponsor may have met certain requirements of the HIPAA Privacy Rule that will permit us to disclose PHI to the plan sponsor. Sometimes the plan sponsor of a group health plan is the employer. In those circumstances, we may disclose PHI to your employer. You should talk to your employer to find out how this information will be used.

Research: We may use or disclose your PHI for research purposes if certain conditions are met. Before we disclose your PHI for research purposes without your written permission, an Institutional Review Board (a board responsible under federal law for reviewing and approving research involving human subjects) or Privacy Board reviews the research proposal to ensure that the privacy of your PHI is protected, and to approve the research.

Required by Law: We may disclose your PHI when required to do so by applicable law. For example, the law requires us to disclose your PHI:

- When required by the Secretary of the U.S. Department of Health and Human Services to investigate our compliance efforts; and
- To health oversight agencies, to allow them to conduct audits and investigations of the health care system, to determine eligibility for government programs, to determine compliance with government program standards, and for certain civil rights enforcement actions.

Public Health Activities: We may disclose your PHI to public health agencies for public health activities that are permitted or required by law, such as to:

- prevent or control disease, injury or disability;
- maintain vital records, such as births and deaths;
- report child abuse and neglect;
- notify a person about potential exposure to a communicable disease;
- notify a person about a potential risk for spreading or contracting a disease or condition;
- report reactions to drugs or problems with products or devices;
- notify individuals if a product or device they may be using has been recalled; and
- notify appropriate government agency(ies) and authority(ies) about the potential abuse or neglect of an adult patient, including domestic violence.

Health Oversight Activities: We may disclose your PHI to a health oversight agency for activities authorized by law, such as: audits; investigations; inspections; licensure or disciplinary actions; or civil, administrative, or criminal proceedings or actions. Health Oversight agencies seeking this information include government agencies that oversee: (i) the health care system; (ii) government benefit programs; (iii) other government regulatory programs; and (iv) compliance with civil rights laws.

Lawsuits and Other Legal Disputes: We may disclose your PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process once we have met all administrative requirements of the HIPAA Privacy Rule.

Law Enforcement: We may disclose your PHI to law enforcement officials under certain conditions. For example, we may disclose PHI:

- to permit identification and location of witnesses, victims, and fugitives;
- in response to a search warrant or court order;
- as necessary to report a crime on our premises;

- to report a death that we believe may be the result of criminal conduct; or
- in an emergency, to report a crime.

Coroners, Medical Examiners, or Funeral Directors: We may release PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or to determine the cause of death. We also may disclose, as authorized by law, information to funeral directors so that they may carry out their duties.

Organ and Tissue Donation: We may use or disclose your PHI to organizations that handle organ and tissue donation and distribution, banking, or transplantation.

To Prevent a Serious Threat to Health or Safety: As permitted by law, we may disclose your PHI if we believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

Military and National Security: We may disclose to military authorities the PHI of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials PHI required for lawful intelligence, counter-intelligence, and other national security activities.

Inmates: If you are a prison inmate, we may disclose your PHI to the prison or to a law enforcement official for: (1) the prison to provide health care to you; (2) your health and safety, and the health and safety of others; or (3) the safety and security of the prison.

Workers' Compensation: As part of your workers' compensation claim, we may have to disclose your PHI to a worker's compensation carrier.

To You: When you ask us to, we will disclose to you your PHI that is in a "designated record set." Generally, a designated record set contains medical, enrollment, claims and billing records we may have about you, as well as other records that we use to make decisions about your health care benefits. You can request the PHI from your designated record set as described in the section below called "Your Privacy Rights Concerning your Protected Health Information."

To Your Personal Representative: If you tell us to, we will disclose your PHI to someone who is qualified to act as your personal representative according to any relevant state laws. In order for us to disclose your PHI to your personal representative, you must send us a completed IBC Personal Representative Designation Form or documentation that supports the person's qualification according to state law (such as a power of attorney or guardianship). To request the IBC Personal Representative Designation Form, please contact Member Services at the telephone number listed on the back of your Member Identification card, print the form from our web site at www.ibx.com, or write us at the address at the end of this Notice. However, the HIPAA Privacy Rule permits us to choose not to treat that person as your personal representative when we have a reasonable belief that: (i) you have been, or may be, subjected to domestic violence, abuse or neglect by the person; (ii) treating the person as your personal representative could endanger you; or (iii) in our professional judgment, it is not in your best interest to treat the person as your personal representative.

To Family and Friends: Unless you object, we may disclose your PHI to a friend or family member who has been identified as being involved in your health care. We also may disclose your PHI to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status, and location. If you are not present or able to agree to these disclosures of your PHI, then we may, using our professional judgment, determine whether the disclosure is in your best interest.

Parents as Personal Representatives of Minors: In most cases, we may disclose your minor child's PHI to you. However, we may be required to deny a parent's access to a minor's PHI according to applicable state law.

Right to Provide an Authorization for Other Uses and Disclosures

- Other uses and disclosures of your PHI that are not described above will be made only with your written authorization.
- You may give us written authorization permitting us to use your PHI or disclose it to anyone for any purpose.
- We will obtain your written authorization for uses and disclosures of your PHI that are not identified by this Notice, or are not otherwise permitted by applicable law.

Any authorization that you provide to us regarding the use and disclosure of your PHI may be revoked by you in writing at any time. After you revoke your authorization, we will no longer use or disclose your PHI for the reasons described in the authorization. Of course, we are unable to take back any disclosures that we have already made with your authorization. We may also be required to disclose PHI as necessary for purposes of payment for services received by you prior to the date when you revoke your authorization.

Your authorization must be in writing and contain certain elements to be considered a valid authorization. For your convenience, you may use our approved IBC Authorization Form. To request the IBC Authorization Form, please contact Member Services at the telephone number listed on the back of your Member Identification card, print the form from our web site at www.ibx.com, or write us at the address at the end of this Notice.

Your Privacy Rights Concerning Your Protected Health Information (PHI)

You have the following rights regarding the PHI that we maintain about you. Requests to exercise your rights as listed below must be in writing. For your convenience, you may use our approved IBC form(s). To request a form, please contact Member Services at the telephone number listed on the back of your Member Identification card or write to us at the address listed at the end of this Notice.

Right to Access Your PHI: You have the right to inspect or get copies of your PHI contained in a designated record set. Generally, a "designated record set" contains medical, enrollment, claims and billing records we may have about you, as well as other records that we may use to make decisions about your health care benefits. However, you may not inspect or copy psychotherapy notes or certain other information that may be contained in a designated record set.

You may request that we provide copies of your PHI in a format other than photocopies. We will use the format you request unless we cannot practicably do so. We may charge a reasonable fee for copies of PHI (based on our costs), for postage, and for a custom summary or explanation of PHI. You will receive notification of any fee(s) to be charged before we release your PHI, and you will have the opportunity to modify your request in order to avoid and/or reduce the fee. In certain situations we may deny your request for access to your PHI. If we do, we will tell you our reasons in writing, and explain your right to have the denial reviewed.

Right to Amend Your PHI: You have the right to request that we amend your PHI if you believe there is a mistake in your PHI, or that important information is missing. Approved amendments made to your PHI will also be sent to those who need to know, including (where appropriate) Independence Blue Cross's vendors (known as "Business Associates"). We may also deny your request if, for instance, we did not create the information you want amended. If we deny your request to amend your PHI, we will tell you our reasons in writing, and explain your right to file a written statement of disagreement.

Right to an Accounting of Certain Disclosures: You may request, in writing, that we tell you when we or our Business Associates have disclosed your PHI (an "Accounting"). Any accounting of disclosures will not include those we made:

- for payment, or health care operations;
- to you or individuals involved in your care;
- with your authorization;
- for national security purposes;
- to correctional institution personnel; or,
- before April 14, 2003.

The first accounting in any 12-month period is without charge. We may charge you a reasonable fee (based on our cost) for each subsequent accounting request within a 12-month period. If a subsequent request is received, we will notify you of any fee to be charged, and we will give you an opportunity to withdraw or modify your request in order to avoid or reduce the fee.

Right to Request Restrictions: You have the right to request, in writing, that we place additional restrictions on our use or disclosure of your PHI. We are not required to agree to your request. However, if we do agree, we will be bound by our agreement except when required by law, in emergencies, or when information is necessary to treat you. An approved restriction continues until you revoke it in writing, or until we tell you that we are terminating our agreement to a restriction.

Right to Request Confidential Communications: You have the right to request, in writing, that we use alternate means or an alternative location to communicate with you in confidence about your PHI. For instance, you may ask that we contact you by mail, rather than by telephone, or at work, rather than at home. Your written request must clearly state that the disclosure of all or part of your PHI at your current address or method of contact we have on record could be an endangerment to you. We will require that you provide a reasonable alternate address or other method of contact for the confidential communications. In assessing reasonableness, we will consider our ability to continue to receive payment and conduct health care operations effectively, and the subscriber's right to payment information. We may exclude certain communications that are commonly provided to all members from confidential communications. Examples of such communications include benefit booklets and newsletters.

Right to a Paper Copy of This Notice: You have the right to receive a paper copy of our Notice of Privacy Practices. You can request a copy at any time, even if you have agreed to receive this Notice electronically. To request a paper copy of this Notice, please contact Member Services at the telephone number on the back of your Member Identification Card.

Your Right to File a Privacy Complaint

If you believe your privacy rights have been violated, or if you are dissatisfied with Independence Blue Cross's privacy practices or procedures, you may file a complaint with the Independence Blue Cross Privacy Office and with the Secretary of the U.S. Department of Health and Human Services.

You will not be penalized for filing a complaint.

To file a privacy complaint with us, you may contact Member Services at the telephone number on the back of your Member Identification Card, or you may contact the Privacy Office as follows:

Independence Blue Cross
Privacy Office
P.O. Box 41762
Philadelphia, PA 19101-1762
Fax: (215) 241- 4023
E-mail: Privacy@ibx.com
Phone: (215) 241- 4735

Section 10: Member Authorization Form

Independence Blue Cross

Authorization to Release Information please print

This form is used to release your protected health information as required by federal and state privacy laws. Your authorization allows the Health Plan (your health insurance carrier or HMO) to release your protected health information to a person or organization that you choose. You can revoke this authorization at any time by submitting a request in writing to the Health Plan (contact Member Services for further instructions). Revoking this authorization will not affect any action taken prior to receipt of your written request.

Member Information: (individual whose information will be released)

Name: (First, Middle, Last, Title)		**Date of Birth:** (Month/Day/Year)
Address: (including zip code)		**Telephone Number:** (including area code)
Group Name/Number: (if available)	**Social Security Number:** (optional)	**Member ID Number:**

Health Plan: (organization that will release your information)

I authorize _____ to release my protected health information as described below.
(Health Plan name on your ID card)

Recipient: (person or organization that will receive your information)

Person's Name or Organization:	**Telephone Number:** (including area code)
Address: (including zip code)	**Fax Number:** (including area code)

Description of the Information to be Released: (what type of information will be released)

Check only one box:

❑ **Psychotherapy notes –** Federal law requires an authorization to use or release psychotherapy notes.
If you check this box, you may not check another box below.

❑ **All information related to the provision of and payment for my health care benefits or services.***

❑ **Specific information described below:***

_____
Examples: The claim related to my service on (date); Appeal information related to my claim on (date)

Purpose of Release:

_____
Examples: At my request; To resolve my appeal; To assist with my health insurance services

***NOTE:** State law requires that you give specific permission to release the information below even if you checked a box above. Indicate your permission for the Health Plan to release any of the following information by initialing all that apply.

Genetic Information _____ (Initials) **HIV/AIDS** _____ (Initials)

Substance/Alcohol Abuse _____ (Initials) **Mental/Behavioral Health** _____ (Initials)

Expiration: (when this authorization will end)

This authorization will expire on _____/_____/_____ (mm/dd/yyyy) OR on the occurrence of the following event:

_____
Examples: Until I revoke this authorization; Resolution of a specific issue

Approval: (You OR your personal representative must sign and date this form in order for it to be complete.)

I understand that this authorization to release information is voluntary and is not a condition of enrollment in this Health Plan, eligibility for benefits, or payment of claims. I also understand that if the person or organization I authorize to receive the information described above is not subject to federal health information privacy laws, they may further release the protected health information and it may no longer be protected by federal privacy laws.

Member Signature

By signing below, I authorize the use of my protected health information.

_____
(Signature of Member)

_____
(Date)

Personal Representative Information

A personal representative is a person who has the legal authority to act on behalf of an individual. A copy of a Power of Attorney or other court-related legal document must be on file at the health plan.

_____ _____ (_____)_____
(Printed Name of Personal Representative) (Date) (Telephone Number)

_____ _____
(Signature of Personal Representative) (Description of representative's authority)

PLEASE KEEP A COPY OF THIS FORM AND THE INSTRUCTIONS FOR YOUR RECORDS 020703 v2

Independence Blue Cross

Authorization to Release Information

This form is used for you or your personal representative to authorize the Health Plan to release your protected health information to another person or organization at your request.

"Protected health information," means individually identifiable health information. It is information about you, including your name, address and medical information and may relate to your past, present or future physical or mental health or condition. The Health Plan maintains information that may include eligibility, benefits, claims or payment information.

Member Information: (individual whose information will be released)

Print your complete name, address, date-of-birth and telephone number. Provide your group name and number if available. Social Security number is optional.

Important: Provide the Member ID Number located on the front of your Health Plan identification card. Be sure to include any letters in front of the identification number.

Health Plan: (organization that will release your information)

The Health Plan is your insurance carrier or HMO that maintains information about you. Print the name of your Health Plan on the line provided.

Recipient: (person or organization that will receive your information)

The recipient is a person or organization that you choose to receive your protected health information from the Health Plan. You must provide all of the contact information in order for the information to be released.

- Identify the person, family member or organization to receive your information.
- Provide the contact information about the person, family member or organization.

Description of the Information to be Released: (what type of information will be released)

You must indicate or describe the information to be released. **Check one box that best describes your request**. There are three choices. The first choice is **Psychotherapy Notes**. The second choice is **All Information**. The third choice is **Specific Information** that you must describe on the line provided.

If this authorization is to release psychotherapy notes, the Health Plan cannot release any other information unless you complete another Authorization to Release Information form.

Psychotherapy Notes are notes recorded by a mental health professional documenting or analyzing the contents ofa conversation during a private counseling session or a group, joint, or family counseling session. These notes are separated from the rest of the individual's medical record. **Psychotherapy notes cannot be combined with an authorization to release any other type of information.**

All Information. If you check this box the Health Plan may release all information related to the provision of a payment for my health care benefits or services. If someone is directly involved in coordinating your health care or benefits, you may want them to have access to all of your information.

Specific Information. By checking this box you indicates that you want only specific information to be released. Describe the specific information on the line provided.

Purpose of Release. You must provide a brief description of the reason you want this information released. The statement, "At my request" is sufficient.

IMPORTANT: State law requires that you give specific permission to release certain health information. Your initials are required on each line in order for the Health Plan to release information for HIV/AIDS, Substance/Alcohol Abuse, Genetic information or Mental/Behavioral Health information.

Expiration: (when this authorization will end)

Print either an expiration date OR event, but not both. If an expiration event is used, the event must relate to the purpose of the release of information being authorized.

Approval: (You OR your personal representative must sign and date this form in order for it to be complete.)

Member Signature.
If you are the individual whose information will be released, you must sign and date in this section.

Personal Representative Information. If you are the personal representative, the member's signature is not required. However, you must provide the requested information, signature and date. A copy of the legal authority, such as a Power of Attorney or other court-initiated document, must be on file with the Health Plan.

PLEASE KEEP A COPY OF THIS FORM AND THE INSTRUCTIONS FOR YOUR RECORDS 020703 v2