Health Insurance Portability and Accountability Act ("HIPAA")
Privacy and Security Training Manual

Information is one of the Joint Industry Board's ("JIB") most important assets. The JIB is entrusted with the protection of our participants' personal data such as social security numbers, personal health, and personal financial information. We take this responsibility very seriously.

Another valuable asset is you, the JIB employee. During the course of performing your job for the JIB, you may be exposed directly or indirectly to confidential information. It is critical that you understand the policies and procedures concerning such information so that the integrity of the JIB is never compromised and that the trust of the Local 3 membership and all of our participants is always maintained. This can only be achieved through a team effort. Effective privacy and security involves the participation and support of every JIB employee who deals with information or information systems. It is the responsibility of all employees to know and understand the guidelines presented in this booklet, and to conduct their activities accordingly.

The attached JIB HIPAA Privacy and Security Policies and Procedures ("HIPAA Policies") are intended as a training manual for this important topic. Once you have read this document and understand the HIPAA Policies, please sign the attached certificate and return it to either your Supervisor or Human Resources.

Please note that the JIB Security Policies and Procedures can be found on the JIB Intranet.

If you have questions regarding the HIPAA Policies, or if you have suggestions or comments regarding this document, contact the HIPAA Security Officer, Steve Butman, or the HIPAA Privacy Officer, Laura Taylor-O'Boyle.

[This document is meant for training purposes only and does not alter or amend the JIB's Security or Privacy Policies and Procedures in any way.]

OVERVIEW OF PRIVACY POLICIES

Following is an overview of the HIPAA Privacy Rule and the JIB's Privacy Policies and Procedures ("Privacy Policies") that were adopted to ensure that the JIB complies with the Privacy Rule. Following this overview are the actual Privacy Policies, which you should also review.

What Information Needs To Be Protected?

HIPAA restricts the use and disclosure of protected health information ("PHI"). PHI refers to the health and demographic information about an individual that is created or received by a health care provider, health plan, employer or health care clearinghouse that relates to the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or the payment for the provision of health care to an individual.

HIPAA's Privacy Rule establishes standards to protect not only the confidentiality of Protected Health Information, but also the availability and integrity of the information.

However, unless information is created or received by the JIB, it is not PHI, even if it includes medical information. For example, medical information revealed by a participant to a Union business agent or employer is not PHI unless and until it is created or received by the JIB.

Who Is Subject To The Privacy Rule?

The Privacy Rule applies to "covered entities," which includes health care providers, health plans, and various other entities. As the administrator of various health plans affiliated with Local 3, IBEW, the JIB is a "business associate" of the health plans. Just like a covered entities, a business associate such as the JIB is required to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request (see Business Associate Policy).

As an employee of the JIB, you are required to comply with the Privacy Rule and the JIB's Privacy Policies.

What Types Of Uses And Disclosures Of PHI Are Permitted?

The JIB is permitted to use and disclose PHI for treatment, payment or health care operations ("TPO"). In general, this means those uses and disclosures that are necessary for the JIB's operations. The use or disclosure must be limited to the ***minimum necessary*** to accomplish the purpose of the use or disclosure (see Minimum Necessary Policy).

Authorization must be obtained for ALL uses and disclosures other than TPO and for certain other limited purposes, such as public health, or law enforcement (see the following policies: Right to Request Restrictions on Use and Disclosure, Right to Accounting of Disclosures of PHI, Right to Request Transmittal of Communications and/or Payment at Alternate Address, Right to Access to PHI, Verification).

Individual Rights

HIPAA gives individuals certain rights as well. For instance, an individual has the right to have the JIB amend certain information in his or her record (see Right To Amend PHI Policy). In addition, an individual has a right to request and receive an accounting for some disclosures of PHI (see Right to Accounting of Disclosures of PHI). In addition, an individual has the right to review and obtain copies of his or her PHI in certain circumstances (see Right to Access to PHI Policy).

Complaints, Sanctions, and Breaches

If the JIB denies an individual's request to access or make an amendment to his or her PHI, it will inform the individual of the mechanism for the individual to submit a complaint (see Complaint Policy).

The JIB imposes sanctions against its employees who violate the Privacy Rules (see Sanctions for violations of Privacy Rules Policy).

The JIB has implemented a policy for addresses unauthorized use or disclosure of PHI (see Breach Policy).

Whose oversees all of this?

The JIB has designated Laura Taylor-O'Boyle as the Privacy Officer. The Privacy Officer has the primary responsibility for ensuring compliance with HIPAA and will process individual requests, receive complaints, and document personnel training. The Privacy Officer also investigates reports of breaches of unsecured PHI, conduct risk assessments if necessary and appropriate, and manage the provision of notices to affected individuals, the government, and media, as necessary.

[This document is meant for training purposes only and does not alter or amend the JIB's Security or Privacy Policies and Procedures in any way.]

AUTHORIZATIONS

Policy

The Joint Board shall obtain Authorization Forms from a Participant or an eligible dependent (an "Individual") who is covered by a group health plan administered by the Joint Board before disclosing PHI to any individual or entity not otherwise permitted by the Joint Board's procedures or by the Privacy Rule.

Procedures

A. An Authorization is not required for:

1. uses or disclosures of PHI for treatment, payment or health care operations;

2. disclosures to the individual who is subject of the information; or

3. as otherwise permitted under the Privacy Rule and as explained in the Joint Board's Notice of Privacy Practices.

B. An Authorization is required for disclosures to any third party requested by an Individual.

C. The Joint Board must obtain an Authorization for the use or disclosure of psychotherapy notes except for the following:

1. Use or disclosure by Plan to defend a legal action or other proceeding brought by the individual;

2. Use or disclosure to the Secretary of HHS regarding compliance with the HIPAA Privacy Rule;

3. Use or disclosure as required by law;

4. Use or disclosure for health oversight activities with respect to the oversight of the originator of the notes;

5. Use or disclosures to coroners and medical examiners;

6. Uses or disclosures, consistent with applicable law and standards of ethical conduct, where the Joint Board in good faith believes the use or disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person to the public; and is to a person reasonably able to prevent or lessen the threat, including the target of the threat.

D. The Privacy Officer will make the determination whether a specific situation requires an Authorization Form.

E. Individuals must submit the Joint Board's Authorization Form to the Privacy Officer.

F. An Authorization form shall be void if it contains any of the following defects:

1. The expiration date or event has passed;

2. The Authorization was not filled out completely; or

3. The Authorization contains material information known to the Privacy Officer to be false.

4. The Authorization fails to specifically define the PHI to be disclosed.

5. The Authorization is not notarized.

G. Treatment, payment, enrollment, or eligibility for benefits shall not be conditioned on an Individual's provision of an Authorization Form, except in the provision of health care solely for the purpose of creating PHI for disclosure to a third party (e.g., pre-employment physicals and laboratory testing, including drug tests for the JATC/Apprenticeship Program and Members' Assistance Program).

H. The Joint Board shall provide an Individual with a copy of his or her signed Authorization Form.

I. An Individual may cancel his or her Authorization at any time, provided that the cancellation is submitted in writing to the Privacy Officer, on the Cancellation Authorization Form.

J. The Privacy Officer shall retain signed Authorizations and cancellations for at least 6 years from the date of expiration.

K. Authorizations will be used to disclose the PHI of a deceased individual for a period of 50 years following the individual's death. The authorization shall be executed by the personal representative of the deceased. After 50 years have passed, the individually identifiable information of the decedent will no longer be PHI, and as such, an authorization will no longer be needed to disclose that information.

COMPLAINTS

Policy

The Joint Board's policy is to accept and investigate complaints made by a Participant or an eligible dependent who is covered by one of the group health plans the Joint Board administers, or others, including employees, either directly to the Joint Board's Privacy Officer or to the Secretary of the Department of Health and Human Services (the "Secretary").

Procedures

A. If the Joint Board denies an Individual's request to access or to make an amendment, in whole or in part, to PHI, the Joint Board will include in its denial letter to the Individual a description of how the Individual may complain to the Joint Board or to the Secretary.

Internal Complaints

B. Complaints shall be made in writing to the Joint Board's Privacy Officer and must describe acts or omissions that allegedly constitute violations of the Privacy Rule or the Joint Board's privacy practices. If a member of the office staff receives an oral complaint, the staff member shall inform the individual that complaints must be in writing to the Privacy Officer.

C. The Privacy Officer shall investigate complaints regarding the Joint Board's privacy practices, including the Breach Policy.

D. The Joint Board shall not retaliate against any individual who files a complaint with the Joint Board.

E. The Privacy Officer shall report findings to the Administrator for appropriate action.

F. The Joint Board must retain all complaints and their dispositions for at least six years from the date the complaint was created.

DISCLOSURES OF PHI TO INDIVIDUALS INVOLVED IN HEALTH CARE OR PAYMENT OF HEALTH CARE FOR NOTIFICATION OR IN DISASTER RELIEF EFFORTS

Policy

The Joint Board may disclose to a person involved in the health care of a Participant or eligible dependent PH directly related to that person's involvement in the health care of the Individual, or for notification purposes.

The Joint Board may also disclose or use PHI to notify, or assist in the notification of, including identifying or locating, a family member, a Personal Representative of an Individual, or another person responsible for the care of an Individual of an Individual's location, general condition, or death.

The Joint Board may disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities uses and disclosures for notification purposes to a family member, a Personal Representative or another person responsible for the care of an Individual.

Procedures

A. The Joint Board shall recognize the following persons as those involved in health care and/or payment of an Individual:

   1. Spouses; and

   2. Dependent/immediate family;

   3. Any other person that an Individual designates on the "Disclosure for Involvement in Care and Notification Form".

B. For the purpose of sending Explanation of Benefits ("EOBs"), the Joint Board shall deem the Participant to be a person involved in an eligible dependent's health care payment, and, accordingly, shall send all EOBs and other payment-related correspondence pertaining to a Participant and any eligible dependent covered under one of the health plans the Joint Board administers to the Participant.

C. If a Participant designates an authorized representative to act on the Participant's behalf in accordance with the Joint Board's claim and appeal procedures, the Joint Board shall disclose PHI related to that appeal to that designated representative.

D. The Joint Board shall speak to persons authorized, under State or other applicable law to act on behalf of an Individual in making health care related decisions, in accordance with its "Policy and Procedures on Personal Representatives."

E. If the Joint Board is using or disclosing PHI for disaster relief purposes, the Joint Board needs to comply with the procedures set forth in paragraphs F and G to the extent that the Joint Board, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

F. The Joint Board may use or disclose PHI to a person involved in on Individuals health and/or payment for health care if it:

1. Obtains the Individual's agreement; or

2. Reasonably infers from the circumstances, based on the exercise of professional judgment that an Individual does not object to the disclosure to an appropriate party. For example, when an Individual brings a spouse into a doctor's office when treatment is being discussed.

3. If an Individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of an Individual's incapacity or an emergency circumstance, the Joint Board, in the exercise of professional judgment, may determine whether the disclosure is in the best interests of an Individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with an Individual's health care or payment of health care.

G. If the Joint Board suspects that an incapacitated Individual is a victim of domestic abuse and that the person seeking information about an Individual may have abused him or her, the Joint Board shall not disclose information to the suspected abuser if there is reason to believe that such a disclosure could cause an Individual serious harm.

H. The Medical Department may use professional judgment to make reasonable inferences of an Individual's best interest in allowing a designated person to act on behalf of an Individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

I. The Joint Board need not verify the identity of a family member, spouse or other person involved in a person's health care or payment of health care pursuant to the Joint Board's policy and procedures on "Verification of Identity and Authority of Individuals and Entities Requesting PHI." An Individual's act of involving the other persons in his or her care suffices as verification of his or her identity. In such an instance, the Joint Board need not use a verification process.

J. The Joint Board may disclose a decedent's PHI to a family member, other relative, or close personal friend of the decedent, or any other person

previously identified by the decedent to the Joint Board if the disclosure is directly relevant to such person's involvement with the decedent's care or payment related to the decedent's health care, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to the Joint Board. The Joint Board will comply with the terms of this policy and procedure with respect to the PHI of a decedent for a period of 50 years following the date of such decedent's death. After 50 years have passed, the individually identifiable health information of the decedent is no longer PHI protected by the privacy rules.

JOB DESCRIPTION FOR PRIVACY OFFICIAL

The Privacy Officer's responsibility includes the following:

A. Overseeing the development and implementation of the Joint Board's Policies and Procedures, in coordination with counsel and senior management of the Joint Board.

B. Arranging training programs for the staff of the Joint Board, the Trustees, and, where appropriate, business associates.

C. Arranging for the distribution of the Privacy Notice.

D. Overseeing the preparation or amendment of business associate contracts.

E. Overseeing the development and implementation of appropriate physical, administrative and technical safeguards of PHI held by the Joint Board.

F. Processing requests for accountings of disclosures of PHI pursuant to the Policy on Requests for Accounting of Disclosures.

G. Processing requests by Individuals to exercise their individual rights as set forth in the various Policies and Procedures.

H. Processing complaints concerning the Joint Board's compliance with its policies and procedures or with the requirements of the Privacy Rule.

I. Cooperating with the Office of Civil Rights or other applicable governmental agency in any compliance review or investigation.

J. Providing information about matters covered by the Notice.

K. Implementing the Joint Board's documentation retention policy, including determining when and how to retain documents.

L. Reporting to the Joint Board's Administrator.

M. With regard to reports of breaches of unsecured PHI, investigating such reports, conducting risk assessments if necessary and appropriate, and managing the provision of notices to affected individuals, HHS and the media, as necessary and appropriate.

MINIMUM NECESSARY

Policy

When using or disclosing PHI or when requesting PHI from another covered entity, such as another plan, a provider or a clearinghouse, or a Business Associate, the Joint Board shall make reasonable efforts to limit the PHI used, disclosed or requested to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
The Joint Board shall make reasonable efforts to limit the access to PHI of persons or classes of persons in the Joint Board's workforce who need to use or disclose PHI to carry out their duties to the minimum necessary PHI which is needed.
The Joint Board shall implement policies and procedures that identify routine and recurring disclosures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. Non-recurring and non-routine requests of disclosures will be referred to the Privacy Officer for disposition.
The minimum necessary standard does **not** apply to the following uses or disclosures:

- disclosures to or requests for disclosure by a provider;
- disclosures made to a Participant or eligible dependent;
- disclosures made pursuant to an Authorization;
- disclosures required or permitted to be made to the Secretary of Health and Human Services under the HIPAA Privacy Rule;
- uses or disclosures that are required by law; and
- uses or disclosures that are required for compliance with the HIPAA Privacy Rule.

Procedures

A. The Joint Board has determined that access to PHI will be limited by job description and function and access to PHI will be granted on the basis of "need-to-know" to perform a specific job function, as specified in the attached listing.

B. The Joint Board has identified for each such person or class of persons listed below the category or categories of PHI to which access is needed and all conditions appropriate to such access:

Recipient	**Record Set (category of PHI)**	**Purpose**
Mail clerks	Paper claim and other related documentation EOB Payment Checks	Claims separation; envelope stuffing; copying; scanning; storage
Information Processing Department	Claims System Paper claim and other related documentation Documentation from Providers	Processing claims; Participant inquiry; provider inquiry; business associate inquiry
Administrator, Benefits	Claims System	Claims review; Adjustment

Manager and other Management-level Employees	Paper claim and other related documentation Documentation from Providers	to claims; Internal Audit; Cost containment
Accounting Department	Remittance and payroll reports Eligibility and Enrollment Records Register of approved bills	Payment and discovery of payment error
Members' Records	Dental benefits & prescription drug claims System Dental benefits & prescription drug paper claims and other related documentation Documentation from Providers Remittance and payroll reports and other related documentation	Eligibility confirmation; Participant Inquiry; Monitor payment
Members' Assistance Program	Claims System Paper claim and other related documentation Documentation from Providers	Eligibility confirmation
Director of Medical Department or other Medical Department Staff	Claims System Paper claim and other related documentation Documentation from Providers	Medical Necessity determination; medical review
Hospitalization Dept.	Claims System Paper claim and other related documentation Documentation from Providers	Processing claims; Participant inquiry; provider inquiry; business associate inquiry

C. All members of the workforce who require access to PHI for the purpose of performing their job functions shall receive training regarding the Joint Board's minimum necessary policy and procedures, and must sign a non-disclosure agreement.

D. The Joint Board shall protect PHI and limit access as appropriate in accordance with its "Policy and Procedure on Safeguards for the Protection of PHI " and other security measures which the Joint Board shall adopt.

E. If the Joint Board retains temporary workers to assist in payment and health care operations, such workers will be informed of the Joint Board's privacy policies and asked to sign a non-disclosure agreement. Temporary worker access to information will be monitored and controlled.

F. The Joint Board shall not disclose an Individual's entire medical record in fulfillment of any request subject to the minimum necessary standard except where the Privacy Officer determines that specific justification of

such disclosure is reasonably necessary to accomplish the purpose of the disclosure and such a disclosure is documented.

G. Doctors and nurses in the Medical Department shall have access to the entire medical record for the purpose of treating an Individual.

Routine and Recurring Disclosures

A. For any type of disclosure that the Joint Board makes on a routine and recurring basis, the Joint Board will apply the following policies and procedures:

RECIPIENT	1. **CATEGORIES** **2. AMOUNT OF PHI**	**PURPOSE**
Providers	Eligibility information Benefit coverage level Benefit pre-determination	Facilitate a participant's receipt of treatment
Business Associates that perform pre-authorizations	Eligibility Information Name SSN Dates of Service Provider/Place of Service	Confirm that participant pre-authorized treatment when Claim System does not indicate pre-authorization
Appeals Committees (Trustees, Counsel, Staff)	Medical records Previously submitted pre-determinations Documentation needed to decide appeal	Decide payment or denial of payment by Plan
Outside expert medical reviewers	Diagnosis Codes Provider Notes Medical records	Determine medical necessity of services
Prescription Benefit Managers	Name SSN Eligibility Information Date of birth	Immediate System update
PPO Networks	Name SSN Dates of Service Provider/Plan of Service Diagnosis Codes Procedure Codes Eligibility Information	Re-price and pay claims; Periodic system update
Outside Auditors	Claims Findings report Documentation needed to facilitate the audit	Audit required by law
Judicial and Administrative	Any information requested	Required by law

Proceedings; Entities Authorized by Law		
Outside Attorneys	Remittance reports Documentation needed to assist Trustees in deciding an appeal Documentation needed to render an opinion	To perform legal services

B. The Joint Board may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

1. making disclosures to public officials that are permitted under the Privacy Rule, if the public official represents that the information requested is the minimum necessary for the stated purpose;

2. the information is requested by another health plan, provider, or clearinghouse; or

3. the information is requested by a professional who is a member of a Joint Board's workforce or is a business associate of the Joint Board for the purpose of providing professional services to the Joint Board, if the professional or Business Associate represents that the information requested is the minimum necessary for the stated purpose.

The disclosure would be considered a routine disclosure and the Privacy Officer would not have to review it. However, if the request is vague or overbroad, the Joint Board may seek clarification before responding.

Non-Routine and Non-Recurring Disclosure

A. For disclosures that do not occur on a routine or recurring basis, the Joint Board will apply the following criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.

1. The non-routine disclosure must be necessary to allow the group health plans that the Joint Board administers to carry out its obligations under ERISA and the governing plan documents and the law.

2. The non-routine disclosures must be otherwise consistent with the Joint Board's privacy policies, and not prohibited by the Privacy Rule.

3. A request for a non-routine disclosure that is accompanied by an individual's written authorization that is compliant with HIPAA will be honored in a manner consistent with the Joint Board's privacy policies.

B. The Joint Board's Privacy Officer will review requests for all non-routine and non-recurring disclosures on an ***individual basis*** in accordance with the Joint Board's criteria.

PERMITTED USES AND DISCLOSURES OF PHI THAT DO NOT REQUIRE INDIVIDUAL AUTHORIZATIONS OR AN OPPORTUNITY TO AGREE OR OBJECT

Policy

The Joint Board may use and disclose only the minimum necessary amount of PHI for the following purposes, without providing an opportunity to agree or object, and without obtaining the authorization of a Participant or an eligible dependent who is covered by the one of the group health plans it administers:

A. Required by Law – The Joint Board, including the Medical Department, may use or disclose PHI to the extent that such use or disclosure is required by federal, state or local law. If the use or disclosure is to report abusive situations, to comply with judicial or administrative legal process, or for law enforcement purposes, the use or disclosure must also comply with these policies and procedures.

B. Public Health Activities – The Medical Department may disclose PHI to public health authorities that are authorized by law to collect or receive PHI for the purposes of

- Controlling disease, injury or disability;
- Reporting of disease, injury, vital events such as birth or death;
- Conduct of public health surveillance, investigations and interventions.

The Joint Board may also, at the direction of a public health authority, disclose PHI for the above-listed purposes to an official of a foreign government agency that is acting in collaboration with a public health authority.

C. Child Abuse & Neglect – The Joint Board may disclose PHI to any public health authority authorized by law to receive reports of child abuse or neglect.

D. Food and Drug Administration – The Joint Board may disclose PHI to a person or company subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include: (A) to collect or report adverse events, product defects or problems (e.g. labeling), or biological product deviations; (B) to track FDA-regulated products; (C) to enable product recalls, repairs or replacement, or lookback; or (D) to conduct post-marketing surveillance.

E. Communicable Diseases – – The Joint Board may disclose PHI to a person who may have been exposed to a communicable disease or may otherwise

be at risk of contracting or spreading a disease or condition, if the Medical Department is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

F. Health Oversight Activities – The Joint Board, including the Medical Department, may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, investigations, inspections, and legal proceedings and actions. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights law.

G. Coroners, Medical Examiners and Funeral Directors – The Joint Board, including the Medical Department, may disclose an Individual's PHI to a coroner or medical examiner for identification purposes, or other duties authorized by law. The Joint Board, including the Medical Department, may also disclose PHI to a funeral director, as authorized by law, in order to permit the funeral director to carry out his/her duties.

H. Cadaveric Organ, Eye or Tissue Donation – The Joint Board may use or disclose PHI to organ procurement organizations or other entities engaged in procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

I. Disclosures to Avert a Serious Threat to Health or Safety- The Medical Department may disclose PHI, if in good faith, it believes it to be necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public. Such disclosure must be to a person able to prevent or lessen the threat, including the target of the threat. The Medical Department may also disclose information, if in good faith, it believes that it is necessary for law enforcement authorities to identify or apprehend an individual who the Joint Board reasonably believes may have caused serious physical harm to the victim, because of a statement by an individual admitting participation in a violent crime. In this situation, the Medical Department may only disclose the following: (a) name and address; (b) date and place of birth; (c) social security number; (d) ABO blood type and rh factor; (e) type of injury; (f) date and time of treatment; (g) date and time of death, if applicable; and (h) a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars and tattoos.

The Medical Department may not disclose for the purposes of identification or location any PHI related to the individual's DNA or DNA analysis, dental records, or typing, sampling or analysis of body fluids or tissue. The Medical Department may also disclose when it is necessary for law enforcement to

identify or apprehend an individual who is believed to have escaped from a correctional institution or lawful custody.

J. Specialized Government Functions

1. *Military and Veterans Activities* – The Joint Board may use and disclose the PHI of Armed Forces personnel for activities deemed necessary by appropriate military command authorities or to a foreign military authority if the Individual is a member of that foreign military service.

2. *National Security and Intelligence Activities* – The Joint Board may disclose PHI to authorized federal officials for the conduct of lawful national security and intelligence activities.

3. *Protective Services for the President and Other* – The Joint Board may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by federal law, or to foreign heads of state or other persons authorized by federal law.

K. Correctional Institutions and Related Law Enforcement Custodial Situations - The Joint Board may disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate or other person who is the subject of the PHI if the correctional institution or such law enforcement official represents that such information is necessary to provide the Individual with health care; to protect the health and safety of the Individual or others; or for the security of the correctional institution. These rules do not apply if the Individual is no longer an inmate, released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

L. Workers' Compensation – The Joint Board may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

Procedures

A. The Joint Board shall train its workforce members on the policies and procedures listed above.

B. All questions concerning whether a use or disclosure is permitted without authorization or allowing an Individual an opportunity to agree or object should be addressed to the Privacy Officer. The Joint Board may reserve the right to make the disclosure or to seek legal guidance regarding whether the disclosure should be made.

C. The Joint Board shall document and retain for six years the following:

1. The date of the disclosure of any of the foregoing;

2. The name and address, if known, of the entity or person who received the PHI;

3. A brief description of the PHI disclosed;

4. A brief statement of the purpose of the disclosure;

D. The Joint Board shall temporarily suspend an Individual's right to receive of an accounting of disclosures to health oversight agencies if the agency provides the Board with a ***written*** statement as to why the accounting would impede the investigation and specify the length of time the suspension is required.

LEGAL PERSONAL REPRESENTATIVES

Policy

Where a person is authorized, under State or other applicable law to act on behalf of a Participant or eligible dependent covered under a group health plan administered by the Joint Board in making health care related decisions, the Joint Board shall, except in limited situations discussed below, treat that person as the Legal Personal Representative of the Individual with respect to uses and disclosures of the Individual's PHI, as well as the Individual's rights under the Privacy Rule.

Procedures

Persons the Joint Board Shall Recognize as an Individual's Legal Personal Representatives

A. The Joint Board shall determine whether a person is a Legal Personal Representative of a living Individual based on state or other applicable law, and, if necessary, consult with counsel.

B. The Joint Board shall recognize the following as an Individual's Legal Personal Representative:

1. A person with legal authority to make health care decisions on behalf of the Individual (*e.g.*, health care power of attorney, court appointed legal guardian, general power of attorney) if an Individual is an adult or emancipated minor;

2. A parent, guardian or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child, subject to exceptions discussed below, if an Individual is an unemancipated minor; and

3. A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions), such as the executor of the estate, next of kin or other family member, or durable power of attorney, if an Individual is deceased.

Notwithstanding the above, the Joint Board will not provide PHI, other than payment information, to a parent or other Legal Personal Representative of a child 12 years or older without a written request from the parent or other Legal Personal Representative.

C. Where a Legal Personal Representative has broad authority to act on behalf of a living individual in making decisions related to health, such as a parent or legal guardian of a mentally incompetent adult, the Joint Board shall treat the Legal Personal Representative as an Individual for <u>all</u> purposes under the Privacy Rule.

D. Where a Legal Personal Representative's authority is limited or specific to health care decisions, the Joint Board shall treat the Legal Personal Representative as the Individual only with respect to PHI that is relevant to the representation. For instance, a person with a limited health care power of attorney regarding only a specific treatment, such as lung cancer, is an Individual's Legal Personal Representative only with respect to PHI that relates to that health care decision.

E. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a decedent for a period of 50 years following the date of such decedent's death. After 50 years have passed, the individually identifiable health information of the decedent is no longer PHI protected by the privacy rules.

Exceptions to the General Rule that Parents are the Legal Personal Representatives of Their Minor Children

A. In the following circumstances, the Joint Board shall NOT treat a parent as a Legal Personal Representative of a minor child(ren):

1. Where the minor obtained a particular health care service without a parent's consent as permitted by applicable state or other law (as referenced in the attached chart "State Law Survey on Minors");

2. Where a court determines or other law authorizes someone other than the parent to make a treatment decision for a minor;

3. Where a parent agrees to a confidential relationship between a minor and a physician.

B. Where a law is silent or not clear concerning parental access, the Joint Board may use its discretion to provide or deny a parent access consistent with state law, and the decision shall be made by a licensed health care professional in the exercise of professional judgment.

C. Regardless of whether a parent is a Legal Personal Representative of a minor, the Joint Board may disclose to a parent, or provide the parent access to, a minor child's PHI when and to the extent it is expressly permitted or required by State or other laws (including relevant case law).

Abuse, Neglect and Endangerment Situations

A. If the Joint Board reasonably believes that an Individual, including a minor, has been or may be subjected to domestic violence, abuse or neglect by a Legal Personal Representative, or that treating a person as an Individual's Legal Personal Representative would endanger an Individual, the Joint Board may choose not to treat the person as the Individual's

Legal Personal Representative, if in the exercise of professional judgment, doing so would not be in the best interest of an Individual.

B. The Joint Board shall verify a Legal Personal Representative's authenticity pursuant to its policy and procedures on "Verification of Identity and Authority of Individuals and Entities Requesting PHI."

SAFEGUARDS FOR THE PROTECTION OF PHI

Policy

The Joint Board on behalf of all of the group health plans it administers and the Medical Department of the Hospitalization Benefit Plan shall reasonably safeguard Participant's or Eligible Dependent's PHI from any intentional or unintentional use or disclosure that is in violation of the Privacy Rule or the Joint Board's policies and procedures, and shall limit incidental uses and disclosures made pursuant to an otherwise permitted or required use or disclosure.

Procedures

A. The Joint Board will designate security protocols for electronic or paper documents (including reporting a breach of privacy and disciplinary procedures for employees that breach privacy policies.)

B. All staff members of the Joint Board who perform functions requiring contact with PHI will receive appropriate training on the Joint Board's privacy policies and procedures including the specific methods to be used to secure PHI while in use or storage.

C. Access to physical areas where participants' and eligible dependents' PHI is located shall be limited to staff members to those who have a business purpose for such information.

D. The Joint Board has the right to monitor both internal and external e-mails. E-mail shall be used for appropriate business purposes.

E. The Joint Board will provide each claim handler requiring access to PHI with sufficient workspace storage capacity to secure the PHI during work and after work hours.

F. Paper claims should be stored in a file cabinet that is locked when not in use. No files containing PHI should be left out on a desk overnight.

G. The Joint Board will employ appropriate password and other similar protections to secure electronic PHI.

H. The Joint Board will maintain sufficient on and off-site storage capacity to ensure that all PHI while maintained by the Joint Board is secured when not in active use.

I. The Joint Board has created a written disaster recovery program for loss of data due to fire, vandalism, natural disaster, or other system failure.

J. The Privacy Officer will periodically assess the Joint Board's administrative, physical and technical safeguards to make any necessary

and appropriate modifications to continue to reasonably safeguard PHI from any intentional or unintentional use or disclosure.

SANCTIONS FOR VIOLATION OF PRIVACY RULES

Policy

It is the policy of the Joint Board to impose sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Joint Board, or with the requirements of the Privacy Rule, including the Breach Policy

Procedure

A. All members of the Joint Board's workforce are required to report to the Privacy Officer any conduct by co-employees perceived to be violations of the Privacy Rule, including the Breach Policy.

B. The Privacy Officer shall conduct an investigation to determine whether disciplinary misconduct occurred.

C. Disciplinary or corrective action for misconduct and/or violations of the Joint Board's privacy policies and procedures or the requirements of the Privacy Rule, including the Breach Policy, will be imposed up to and including termination.

D. The Joint Board shall document the sanctions imposed, if any, for at least six years.

Exceptions to Applying Sanctions

Disclosures in Pursuit of HIPAA Enforcement

The Joint Board shall not retaliate against any member of its workforce who:

1. files a complaint with the Secretary of HHS;

2. testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing; or

3. opposes any act or practice made unlawful by the Privacy Rule, provided that the person has a good faith belief that the practice is unlawful, and the manner of the opposition is reasonable and does not involve the disclosure of PHI in violation of the Privacy Rule.

VERIFICATION

Policy

Before the Joint Board discloses PHI of a Participant or an eligible dependent covered by one of the health plans administered by the Joint Board, including for treatment, payment,

and operations, the Joint Board shall verify the identity and authority of the requestor where the Joint Board does not know the person requesting the PHI. Knowledge may take the form of a known place of business, address, phone or fax number or human being.

Where documentation, statements or representations, whether oral or written, from the person requesting the PHI are a condition of disclosure, the Joint Board shall obtain these documentation, statements, or representations prior to disclosing the requested information. Additional verification shall only be required where the Privacy Rules or other law requires additional proof of authority or identity.

The Joint Board shall not verify the identities and authority of an Individual, business associates, or other entity that is known to the Joint Board.

Procedures

When Verification is Not Required

A. The Joint Board may disclose PHI to prevent or lessen a serious and imminent threat to the health or safety of a person or the public if disclosure is made to a person reasonably able to prevent or lessen the threat. The Joint Board shall not demand written proof that the person requesting the PHI is legally authorized; verbal representations are sufficient.

B. The Joint Board shall not require verification of identity for persons assisting in an Individual's care or for notification purposes. All uses and disclosures for these purposes shall be consistent with the Joint Board's policy and procedures regarding "Uses and Disclosures for Involvement in an Individual's Care and for Notification Purposes."

C. The Joint Board shall not require verification of identity for disclosures of PHI to disaster relief organizations under certain emergency situations.

When Verification is Required

A. Individuals Requesting Their Own PHI

1. In-Person Requests: The Joint Board shall verify the identity of the Individual by requesting that he or she complete the "Request for Information" form.

2. Requests by Telephone: The Joint Board shall verify the identity of the Individual by requiring that he or she provide one of the following: social security number, date of birth, or union card number. Employees of the Joint Board shall follow the procedures set forth in the Caller Disclosure Grid.

3. Requests by Mail or Fax: The Joint Board shall verify the identification of the Individual by requesting that the Individual provide his or her social security number.

B. Requests on Behalf of Another

1. The Joint Board shall only disclose PHI to an individual requesting information on behalf of a Participant or an eligible dependent who is covered by the Joint Board if the requestor is the Personal Representative of the Participant or eligible dependent, as set forth in the Joint Board's policy and procedures regarding Personal Representatives. The Personal Representative shall submit the appropriate legal form (*e.g.*, a valid Power of Attorney), if applicable.

2. In addition, the Joint Board shall verify the authority and identity of the Personal Representative's relationship to the Individual, in addition to the Personal Representative's identity, for instance, by requiring a parent/guardian to provide a minor's birth certificate. For requests by telephone, employees of the Joint Board shall follow the procedures set forth in the Caller Disclosure Grid.

C. *Requests by Providers:* The Joint Board shall verify the identity of providers by requesting the provider's Tax Identification Number ("TIN"). If the provider does not have a TIN, the Joint Board shall request that the provider a copy of the most recent W-9 Form. Alternatively, the Joint Board may also verify the provider's identity by requiring requests for disclosures to be in writing on the entity's letterhead, or if requested by telephone, by calling back the main entity's switchboard, and following the procedures set forth in the Caller Disclosure Grid.

D. *Requests by Public Officials or Persons Acting on Behalf of the Public Official:* When the person requesting PHI is a public official or a person acting on behalf of the public official, the Joint Board may rely on any of the following to verify identity:

1. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

2. If the request is in writing, the request is on appropriate government letterhead; or

3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

When the person requesting PHI is a public official or a person acting on behalf of the public official, the Joint Board may rely on the following to verify authority:

1. A *written* statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority.

2. If a request is made pursuant to legal process, warrant, subpoena, or order issued by a grand jury or a judicial or administrative tribunal, legal authority is presumed to constitute legal authority.

HITECH BREACH POLICY

A. Avoiding, Reporting, and Evaluating Breaches

1. **Avoiding Breaches—**In accordance with the Joint Board's Privacy Policies and *Security Policies* ("Security Policies"), the Joint Board shall take all reasonable and necessary steps to avoid Breaches.

To avoid Breaches, the Joint Board has taken the following steps.

(a) The Joint Board has adopted Security Policies to protect the confidentiality, integrity, and availability of all PHI the Joint Board creates, receives, maintains, or transmits.

(b) The Joint Board has adopted Privacy Policies, *inter alia*, to limit the PHI that is used, disclosed, or requested to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(c) The Joint Board has adopted technologies and methodologies specified by the Secretary in the guidance issued at 74 FR 19006 through 19010 to render PHI unusable, unreadable or indecipherable to unauthorized individuals by encrypting all sensitive information and installing a system to secure PHI in outbound email.

2. For purposes of this Policy, a Breach is defined as:

(a) The acquisition, access, use, or disclosure[1] of PHI described in paragraph (3) below, in a manner not permitted under the Privacy Rule.

(b) which poses a significant risk of financial, reputational, or other harm to the individual. The acquisition, access, use, or disclosure of PHI described in paragraph (1) above is presumed to be a breach unless (i) an exception applies, or (ii) the Joint Board or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment.

(c) For purposes of this paragraph, the PHI includes at least one of the following identifiers regarding the individual:

(i) name;

(ii) date of birth;

[1] The terms "disclose" and "disclosure" shall have the meaning given the term "disclosure" in 45 C.F.R. §160.103. Unless otherwise noted, any term used in this Policy shall have the meaning as defined in 45 C.F.R. §§160 through 164, including the terms PHI, the Secretary, Business Associate, Privacy Rule, Security Rule.

(iii) postal address information (other than town, city, or state);

(iv) telephone number;

(v) fax number;

(vi) electronic mail address;

(vii) Social Security number;

(viii) medical record number;

(ix) health plan beneficiary number;

(x) account number;

(xi) certificate/license number;

(xii) vehicle identifiers and serial numbers, including license plate number;

(xiii) device identifiers and serial numbers;

(xiv) web universal resource locators (URLs);

(xv) internet protocol (IP) address numbers;

(xvi) biometric identifiers, including finger and voice prints; and

(xvii) full face photographic images and any comparable images.

3. Exceptions.

The term "Breach" does not include:

(a) Any unintentional acquisition, access, or use of PHI by a workforce member[2] or person acting under the authority of the Joint Board or a Business Associate, made in good faith and within the scope of authority, which does not result in further use or disclosure in a manner not permitted under the Privacy Rule;

(b) Any inadvertent disclosure by a person who is authorized to access PHI at the Joint Board or a Business Associate to another person authorized to access PHI at the Joint Board or the Business

[2] "Workforce member" shall have the meaning given the term "workforce" in 45 C.F.R. §160.103.

Associate or organized health care arrangement in which the Joint Board participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or

(c) Any disclosure of PHI where the Joint Board or Business Associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

4. Discovery of Breach

(a) For purposes of the timing provisions in this Policy, the Joint Board shall treat a Breach as "discovered" as of the first day on which the Breach is known to the Joint Board, or, by exercising reasonable diligence would have been known to the Joint Board. Similarly, a Breach shall be treated as discovered by a Business Associate as of the first day on which such Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate.

(b) The Joint Board, or, as appropriate, the Business Associate, shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the Joint Board (determined in accordance with the federal common law of agency), or Business Associate. *If the Business Associate is an agent of the* Joint Board*, the* Joint Board *is deemed to have knowledge of the Breach as of the date the Business Associate is deemed to have knowledge.*

5. Reporting Apparent Breaches

If a workforce member or person acting under the authority of the Joint Board believes that an event may constitute a Breach, as defined above, such individual or entity shall report the event (an "Apparent Breach") and any relevant additional information to the Joint Board's Privacy Officer and to the Joint Board's Security Officer in accordance with the Joint Board's Privacy and/or Security Policies.

6. Investigating Apparent Breaches

Pursuant to this Policy and the Joint Board's Privacy and/or Security Policies, upon notification of an Apparent Breach, the Joint Board's Privacy Officer and Security Officer shall take the following steps, documenting all findings and conclusions and retaining all relevant documents for the applicable time period:

(a) Determine if the Apparent Breach falls within the definition of Breach under Section B (1) and (3) above.

(i) If YES: Proceed to paragraph 2 of this section.

(ii) If NO: Document the determination, including the basis therefore. No further action is required under this Policy; however, review Privacy and Security Policies to determine whether other action is required.

(b) Determine if the Apparent Breach satisfies one of the exceptions to the definition of Breach, listed in Section B(4), above, and is therefore not a Breach

(i) If YES: Document the determination, including the basis therefore. No further action is required under this Policy; however, review Privacy and Security Policies to determine whether other action is required.

(ii) If NO: Proceed to paragraph 3 of this section.

(c) **Determine whether the Apparent Breach involves Unsecured PHI.** "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued at 74 FR 19006 through 19010.

(i) If NO: Document the determination, including the basis therefore. No further action is required under this Policy; however, review Privacy and Security Policies to determine whether other action is required.

(ii) If YES**:** Conduct a risk assessment**.**

(1) there is a low probability that the PHI has been compromised. The risk assessment shall be conducted so as to allow the JOINT BOARD time to provide any notices required as a result of any Breach.

(2) As part of the risk assessment, the JOINT BOARD will consider at least the following factors as appropriate:

a. To whom the information was impermissibly disclosed. (For example, whether the entity or person who received or accessed the impermissibly disclosed PHI is also

subject to HIPAA and therefore prohibited from disclosing it.)

b. The nature and extent of PHI impermissibly used or disclosed, including the types of identifiers and the likelihood of re-identification, for example, whether individual names or social security numbers were disclosed or health status or diagnosis disclosed, and if the Apparent Breach involves PHI from which the 16 direct identifiers listed in 45 C.F.R. §164.514(e)(2) have been removed, the extent to which the data set could be re-identified.

c. Whether the PHI was actually acquired or viewed.

d. The extent to which the JOINT BOARD may limit the potential harm that could be caused by the Breach in accordance with the mitigation strategies included in its IT security policies and procedures.

e. If the Apparent Breach involves PHI from which the 16 direct identifiers listed in 45 C.F.R. §164.514(e)(2) have been removed, the extent to which the data set could be re-identified.

(3) If the Apparent Breach involves a Breach reported to the Joint Board by a Business Associate, the Joint Board shall determine whether it is necessary and feasible to conduct its own risk assessment, and, if so, the Joint Board shall conduct a risk assessment as described above.

(4) cannot demonstrate that there is a low probability that the PHI has been compromised based on the risk assessment, , proceed to Section II, *Notifications in Case of Breach.* If the Privacy Official and the

Security Official can demonstrate that there is a low probability that the PHI has been compromised based on the risk assessment, document the determination and the basis therefore. No further action is required under this Policy; however, review Privacy and Security Policies to determine whether other action is required.

(5) The Privacy Officer and the Security Officer shall document the results of the risk assessment and maintain such documentation in accordance with the record retention policy and procedures of the Privacy Procedures.

B. Notifications in Case of Breach

1. General Policy

If the Joint Board discovers, or is notified by a Business Associate of, a Breach of Unsecured PHI, the Joint Board shall notify each individual whose Unsecured PHI has been, or is reasonably believed by the Joint Board to have been, accessed, acquired, or disclosed as a result of the Breach as required by HITECH.
The Joint Board shall provide all notices required by this procedure (hereafter referred to as "Breach Notices"), unless a Business Associate is required by law or agreement to do so.

2. Types of Breach Notices

(a) **Notice To Affected Individuals—**Breach Notices to individuals shall be provided as follows:

(i) Written notification by first-class mail to the individual(s) at his or her last known address or, if he or she agrees to electronic notice and such agreement has not been withdrawn, by electronic mail, unless:

(1) the individual affected by a Breach is a minor or otherwise lacks legal capacity due to a physical or mental condition, in which case, the notice shall be provided to the parent or other person who is the personal representative of the individual;

(2) the Joint Board knows the individual is deceased and has the address of the next of kin or personal representative of the

individual as specified under the Personal Representatives Policy of the Joint Board's Privacy Policies and Procedures, in which case, the Joint Board shall provide written notice by first class mail to either the next of kin or personal representative of the individual; or

(3) there is insufficient or out-of-date contact information that precludes written notification to the individual, in which case, a substitute form of notice reasonably calculated to reach the individual shall be provided, as set forth in the following paragraph, II(B)(1)(b).

(ii) Substitute Notice

(1) If there is insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means, as determined in the discretion of the Joint Board.

(2) If there is insufficient or out-of-date contact information for 10 or more individuals, substitute notice shall

a. be in the form of either a conspicuous posting for a period of 90 days on the home page of the Joint Board's website, or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside; and

b. include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's Unsecured PHI may be included in the Breach.

(3) Substitute notice need not be provided where the Joint Board knows the individual is deceased and there is insufficient or out-of-date contact information that precludes

written notification to the next of kin or personal representative of the individual.

(iii) Written notice may be provided in one or more mailings as information is available to the Joint Board.

(iv) Additional Notice in Urgent Situations. In any case deemed by the Joint Board to require urgency because of possible imminent misuse of the Unsecured PHI, the Joint Board may provide information to individuals by telephone or other means, as appropriate, in addition to the Breach Notice.

(v) The Joint Board shall provide the Breach Notice without unreasonable delay and in no case later than 60 calendar days after the Joint Board's discovery of a Breach.

(vi) A reasonable delay under this policy and procedure shall be limited to the time it takes the Joint Board to conduct a prompt investigation into the incident to collect the information needed to provide the required notice to the individual, including performing, to the extent possible, the risk assessment described in this Policy, above.

(vii) The Breach Notice shall contain the information listed in paragraph II(C) of this Policy, below.

(b) Media Notice

(i) For a Breach of Unsecured PHI involving more than 500 residents of a single state or jurisdiction (such as a county, city or town), the Joint Board shall notify prominent media outlets serving the state or jurisdiction.

(ii) The Joint Board shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach.

(iii) The Breach Notice to the media shall contain the information set forth below in paragraph II(C) of this Policy, below.

(c) **Notice to Secretary—**The Joint Board shall, following the discovery of a Breach of Unsecured PHI, notify the Secretary as following:

(i) For Breaches of Unsecured PHI involving 500 or more individuals, the Joint Board shall provide the notification required by this provision in the manner specified on the HHS Web site contemporaneously with the Breach Notice.

(ii) For Breaches of Unsecured PHI involving fewer than 500 individuals, the Joint Board shall maintain a log or other documentation of such Breaches and, not later than 60 days after the end of each calendar year, provide the notification required by this provision for Breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

3. Content of Breach Notices

(a) All Breach Notices to individuals and to the media required by this Policy shall include, to the extent possible, the following:

(i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

(ii) A description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

(iii) Any steps individuals should take to protect themselves from potential harm resulting from the Breach.

(iv) A brief description of what the Joint Board is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches.

(v) Contact procedures for individuals, which shall include a telephone number, an e-mail address, website, or postal address to contact the Joint Board.

(vi) The Breach Notice shall be, to the extent possible, in plain language.

(b) The Breach Notice shall contain no PHI, including the PHI that is the subject of the Breach, except as necessary to effectuate this Policy.

C. **Notification to Joint Board by Business Associate—**The Joint Board shall require its Business Associates, pursuant to their Business Associate Agreements, to notify the Joint Board of any Breach of Unsecured PHI following discovery by the Business Associate of the Breach, in accordance with the following:

1. The Business Associate shall provide the notification required by this Policy without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach. The parties may, pursuant to the terms of the Business Associate Agreement, agree to a shorter timeframe for such notification. Notwithstanding the foregoing, if the Business Associate is an agent of the Joint Board, the Business Associate shall provide the notification required by this Policy in time to allow the Joint Board to comply with its obligations under this Policy, including the obligation to provide any required notifications of the Breach within 60 days of the Business Associate's discovery. (The Joint Board shall, with the assistance of the Business Associate, determine whether the Business Associate, with respect to the Breach, is an agent of the Joint Board.)

2. The notification required by this subsection shall include, to the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Breach.

3. The Business Associate shall provide the Joint Board with any other available information that the Joint Board is required by this Policy to provide at the time of the notification required by this provision or promptly thereafter as information becomes available.

4. The Joint Board may, pursuant to its Business Associate Agreements or otherwise, require the Business Associate to fulfill the Joint Board's notification obligations under this Policy and to bear the cost of providing any required notices.

5. The Business Associate shall maintain any documentation regarding the Breach required by the Breach Rule.

D. **Law Enforcement Request for Delay**: Any provision in this Policy requiring the Joint Board or Business Associate to provide notice to any individual or entity within a specified time is subject to any contrary direction by a law enforcement officer pursuant to 45 C.F.R. §164.412 as follows:

1. If a law enforcement official states to the Joint Board or Business Associate that a notification, notice, or posting required under these Breach Policies would impede a criminal investigation or cause damage to national security, the Joint Board for Business Associate shall:

2. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

3. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in this provision is submitted during that time.

Additional Joint Board HIPAA Policies

The Joint Board has additional Privacy Policies, which you are welcome to review. If you have any questions about these additional policies, please contact the Privacy Officer.

- BUSINESS ASSOCIATES: The Joint Board shall disclose PHI only to Business Associates who have entered into Business Associate Agreements in accordance with the Joint Board's minimum necessary policy and procedures.

- DISCLOSURES OF PHI FOR JUDICIAL OR ADMINISTRATIVE PROCEEDINGS: The Joint Board may disclose PHI for a judicial or administrative proceeding in response to: (1) an order from a court or administrative tribunal, or (2) a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court of administrative tribunal.

- NOTICE OF PRIVACY PRACTICES DISTRIBUTION: The Joint Board shall provide participants with a Notice of Privacy Practices explaining how the Joint Board will use and disclose participants' and eligible dependents' PHI, and stating the individual's rights and the Joint Board's legal duties with respect to PHI. The Joint Board shall not send the notice to eligible dependents. (The Medical Department shall provide the Notice to patients.)

- RECORD RETENTION: The Joint Board is subject to certain documentation requirements under HIPAA.

- RIGHT TO AMEND PHI: It is the policy of the Joint Board to honor a request by an individual to amend of his or her PHI maintained by the Joint Board or a Business Associate. The Individual has the right to request an amendment of his or her PHI for as long as that information is maintained in the Designated Record Set by the Joint Board. (A "Designated Record Set" means a group of records that comprise the enrollment, payment, claims adjudication, case or medical management record systems maintained by or for the Joint Board.)

- RIGHT TO REQUEST RESTRICTIONS ON USE AND DISCLOSURE: An individual has the right to request that the Joint Board restrict its use or disclosure of the Individual's PHI for treatment, payment or health care operations. The individual may also request that the Plan not disclose PHI to a spouse or other member of the Individual's immediate family who may be involved in the Individual's care or payment of his or her health care, or that it not disclose PHI to notify relevant people about his or her condition, or location.

- RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI: An individual may request an accounting of disclosures of his or her PHI made up to six years prior to the date of the request, not including disclosures for purposes of treatment, payment or health care operations.

- RIGHT TO REQUEST TRANSMITTAL OF COMMUNICATIONS AND/OR PAYMENT AT ALTERNATE ADDRESS: An individual may request communications from the Joint Board be transmitted at an address other than the individual's home address.

- RIGHT TO ACCESS TO PHI: A participant or an eligible dependent who is covered by the plans administered by the Joint Board has the right to inspect and obtain a copy of his or her PHI in the Joint Board's or its Business Associates' Designated Record Set for as long as PHI is maintained.

- TRAINING: It is the Joint Board's policy to provide training to its staff on the Joint Board's policy and procedures regarding PHI as necessary and appropriate for them to carry out their functions.

[This document is meant for training purposes only and does not alter or amend the JIB's Security or Privacy Policies and Procedures in any way.]

Joint Industry Board of the Electrical Industry

Health Insurance Portability and Accountability Act ("HIPAA")
Security Training Manual

Information is one of the Joint Industry Board's ("JIB") most important assets. The JIB is entrusted with the protection of our participants' personal data such as social security numbers, personal health, and personal financial information. ***We take this responsibility very seriously.***

Another valuable asset is you, the JIB employee. During the course of performing your job for the JIB, you may be exposed directly or indirectly to confidential information. It is critical that you understand the policies and procedures concerning such information so that the integrity of the JIB is never compromised and that the trust of the Local 3 membership and all of our participants is always maintained. This can only be achieved through a team effort. Effective security involves the participation and support of every JIB employee who deals with information or information systems. It is the responsibility of all employees to know and understand the guidelines presented in this booklet, and to conduct their activities accordingly.

The attached *JIB Security Policies and Procedures* is intended as a training manual for this important topic. Once you have read this document and understand the JIB HIPAA Security Policies and Procedures, please sign the attached certificate and return it to either your Supervisor or Human Resources.

Please note that the *JIB Security Policies and Procedures* can be found on the JIB Intranet.

If you have questions regarding the JIB's security policies and procedures, or if you have suggestions or comments regarding this document, contact the HIPAA Security Officer, Steve Butman, or the HIPAA Privacy Officer, Laura Taylor-O'Boyle.

What is Information Security?

Information security deals with several different aspects of securing information. Information security is not confined to computer systems or to information in an electronic format. It applies to all aspects of safeguarding information in any of its many forms.

Major items involved in information security include:

• *Confidentiality.* The safekeeping of data and information by restricting access to individuals who have a need, reason, and permission to such data and information.

• *Data Security.* The protection of data in all its forms (electronic, paper, or other), and throughout its life cycle (origination, entry, processing, distribution, storage, and disposal) from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional.

What Information Needs to be Protected?

HIPAA's Security Rule establishes standards to protect not only the confidentiality of Protected Health Information, but also the availability and integrity of the information. Some examples include:

• Protected Health Information (PHI) (e.g. member's and employee's health records, eligibility information). See page 6 for some examples of PHI.

• Electronic Protected Health Information (ePHI) (Protected Health Information that is transmitted electronically).

• Payroll information.

• Account balances.

• Confidential member or employee information (e.g. social security number and address).

Security Guidelines for All Users

The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.

2. Comply with Information Security Policies and Procedures and with all controls established by the owner and custodian of the information.

3. Refer all improper disclosures of PHI both inside and outside of the JIB to HIPAA Privacy Officer, Laura Taylor-O'Boyle. Proper disclosures are those related to treatment, payment, or health care operations. In certain circumstances, the Privacy Officer may specifically delegate the disclosure process to other departments.

4. Keep personal authentication devices (e.g. passwords, SecureCards, personal identification numbers, etc.) confidential.

5. Report promptly to the HIPAA Security Officer, Steve Butman, regarding the loss or misuse of JIB information relating to security.

Treat Paper Records and Electronic Data Equally

Sensitive information on paper is the same as sensitive information on a computer. Both need to be protected from unauthorized access and should be treated with caution and discretion. In particular, protected health information (PHI) in all forms (called ePHI, or Electronic Protected Health Information, when transmitted via computer or other electronic means) is covered by the HIPAA privacy regulations.

Systems Use and Data Ownership

1. Email and internet systems provided by the JIB are intended for JIB-related business use. While personal use of email may be approved on a limited basis as authorized by Management, it should not occur during working time and cannot interfere with job performance. Personal use should not be during working time and should not interfere with job performance. Employees are responsible for exercising good judgment regarding the reasonableness of personal use; however, JIB management reserves the right to determine what constitutes reasonable use and to terminate personal usage rights for employees who abuse their privileges. All employees must obtain approval from their supervisor or manager in order to utilize any equipment for their personal use.

2. Electronic communications through the JIB's information systems are the property of the JIB. The JIB treats all electronic communications sent, received, or stored as business property, including those for personal use.

3. While the JIB's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on JIB systems remains the property of the JIB. No user shall have any expectation of privacy with respect to any electronic message. The JIB monitors all electronic communication and periodically reviews selected messages as part of its audit process.

4. Access to the JIB's equipment is limited to employees who are on site at the JIB or who have

been expressly authorized to access its equipment from other locations. When authorized, access from other locations must be through a secure and encrypted communications channel.
5. The technical staff of the JIB strives to deploy equipment in conformance with the wishes of employees whenever possible. Nevertheless, the JIB reserves the right to deploy equipment in a manner most suitable for its business operations and retains final authority over its installation and configuration.
6. To ensure compliance with this policy, authorized individuals within the JIB may monitor equipment, systems and network traffic at any time.

Workstation and Password Requirements
1. Desktop workstations and laptop computers are for business use at the JIB. No software which is not necessary for business operations may be installed on any computer unless such installation is authorized by management.
2. All PCs, laptops and workstations must be locked with a screensaver when not in use.
3. All desktop and laptop computers owned by the JIB must be equipped with approved virus-scanning software with a current virus database. All desktop and laptop computers *not* owned by the JIB must be equipped with approved virus-scanning software with a current virus database whenever they are attached to a JIB computing network.
4. Because information contained on portable computers is especially vulnerable, laptop users are required to comply with the guidelines set forth in the Section entitled "Laptops" on page 5.
5. Employees are required to keep passwords secure and not to share accounts information with anyone, including IT staff. Passwords must be changed every 45 days at a minimum.

Confidential Information
The JIB requires that all sensitive or vulnerable information be encrypted before it is exchanged with parties outside of the JIB. For further information about data encryption, see section entitled, "Exchanging Confidential Information" on page 6.
Please see pages 8-11 for instructions on sending encrypted email.

Prohibited Activities
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. However, under no circumstances is an employee of the JIB authorized to engage in any activity that is illegal under local, state, federal, or international law. The lists below are not meant to be exhaustive. Instead, they attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities
Prohibited activities include but are not limited to:
1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the JIB.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, e-mail bombs, etc.).
4. Using a JIB computer or other electronic media to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
5. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the employee is not an intended recipient, using another person's password, or logging into a server or account that the employee is not expressly authorized to access, unless these activities are within the scope of regular duties.
6. Circumventing user authentication or security of any host, network or account.
7. Using any program, or sending messages of any kind, with the intent to interfere with, or disable computer equipment of any kind.
8. Providing personal or work-related information about, or lists of, JIB-administered plan participants or JIB employees to parties outside the JIB.
9. The saving of any documents or programs on the local hard drive of any JIB computer, unless such use is authorized by management.

10. Copying data to any external device (floppy drive, CD-ROM drive, USB device, etc.) on any JIB computer, unless such use is authorized by management.

Email and Communications Activities

Prohibited activities include but are not limited to:

1. Emailing unencrypted, confidential information to external parties either in the message body or as an attachment. The email gateway has been configured to detect and reject messages that contain such sensitive information. Confidential information shared with external parties must be encrypted as described in the section entitled "Exchanging Confidential Information" on page 5.
2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. Solicitation of email for any other email address, other than the sender's, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Posting the same or similar messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Saving information from email messages when such messages are accessed from computers outside the JIB (i.e., from home or from any other remote location).

Physical Security

The JIB limits physical access to its property and assets to employees and authorized visitors. JIB employees are required to observe the following guidelines with respect to physical access to the JIB premises and equipment:

1. Employees may not share keys, access cards, or codes for security devices with other employees. If an employee loses a key or access card, or suspects that an access code has been compromised, that employee should contact Human Resources at extension 1316.
2. Employees are prohibited from interfering with any physical security mechanism in place at the JIB. In particular, employees are not to circumvent security devices by, for example, propping open security doors or otherwise interfering with their normal operation.
3. Access to the JIB premises must be approved by management, and visitors to the JIB must be accompanied by a JIB employee at all times. Employees who suspect that an unauthorized person has gained access to JIB property should call security at extension 1121.
4. Access to the secured systems area on the fifth floor is limited to those who require access as part of their job responsibilities. Visitor access to the secured systems area must be approved by the Director of Information Technology.
5. Employees should be aware that access logs to all areas of the building are maintained and periodically audited to ensure compliance with these policies. Employees who violate these policies are subject to disciplinary action as described in the section entitled "*Enforcement and Compliance"* on page 7.

Environmental Safeguards

Ensuring that all computer, network, and telecommuting equipment is physically protected from security threats is essential in order to reduce the risk of unauthorized access, inadvertent or unintentional disclosure of information, loss, modification, or damage to JIB information assets. The following measures should be taken to safeguard against equipment failures and to minimize damage from natural hazards.

This policy outlines physical and environmental controls that are in place within the JIB building generally and the data center specifically.

1. Drinking and eating in the immediate areas of computers is restricted in accordance with the already established JIB policy.
2. Employees should exercise care when cleaning or using solvents on or around computer equipment as it is often very sensitive and can be easily damaged.
3. Controls are necessary to minimize damage from natural hazards such as fire or excess water. For example, flooding can result from breaks in the cooling system or water drainage pipes. Computer equipment must be protected against natural disasters such as fire damage, water damage, or electrical surges.
4. Computer equipment must not be located near any combustible or hazardous areas.
5. Smoke detectors and fire extinguishers must be accessible.

6. Care must be taken to keep electronic storage media away from harmful environmental or magnetic influences. For example, a photo-magnet on a desk could damage a floppy disk or a hard drive in the same vicinity.

Printer/Fax and Document Security

1. Printers and fax machines used to print sensitive JIB data or PHI must be located in a physically secure area, or the printer/fax machine must be attended by the recipient during output.
2. The sender must make every effort to ensure the recipient of sensitive or private data is advised when it is being sent.
3. JIB employees must make every effort to ensure that the correct fax numbers are used. For example, information intended for the medical department should only be sent to the fax machine located in the medical department.
4. At least one person in every department should be designated to collect confidential faxes several times daily.
5. It is the responsibility of the person handling sensitive or confidential documents to ensure the documents are shredded or put in a secure recycling bin when being discarded.

Workstation Usage Guidelines

1. The JIB and its employees shall take reasonable and appropriate steps to ensure that workforce members understand which purposes and functions are authorized on their workstations. Employees are not to use workstations for unauthorized purposes or to perform unauthorized functions.
2. All employees must lock their computer when they leave their workstations unattended for a period of time, such as breaks, visits to the restroom, and any other time they may be called away from their workstations. Computers are locked by using keys Ctrl, Alt, and Delete keys and selecting Lock Computer. Upon returning to the workstation, employees can unlock their computer by using keys Ctrl, Alt, and Delete and logging on by using their desktop password. This will restore the screen to the exact place the user left it when he or she locked the computer. Compliance with this security measure will be monitored, as required by law.
3. All employees must log off from their workstations when their shift is complete.
4. All employees are required to report any unauthorized activity at a workstation to Steve Butman at extension 1552.

Laptops

Laptop computers warrant special consideration because they are used off the premises of the JIB and are not subject to the same physical safeguards as other equipment. Several security policies apply only to laptops:

1. Laptop computers are configured with a biometric device which requires users to register one of their fingerprints before they can use the computer. The biometric device also requires users to enter a strong password for access to the computer. This password is separate from any network password users normally enter while onsite at the JIB. Instructions for using the biometric devices are maintained separately.
2. Laptop computers are configured so that nothing can be written to any local drive or any removable storage medium other than the biometric device. Users are not to take any action in attempt to circumvent this policy. Configuring the laptops in this manner means that the JIB is exposed to minimal risk should the laptop be lost or stolen.

Passwords

Generally, you will have two separate and distinct passwords. One is for your desktop log-on. This enables you to log on to the various network directories used in your daily job performance. Files that are in such programs as Microsoft Word, Excel, Paperclip, and Filemaker are all located on the network. Your second password is for logging on to the mainframe and accessing System 2.

Desktop Passwords

1. Passwords must not consist of commonly recognizable names or words, readily guessable sequences of letters or numbers, or data that can be easily associated with the user, such as birthdays, names of self, spouse, children, etc.
2. Password length must be a minimum of six characters. Where feasible, 8-10 characters will strengthen password security.
3. The same password must not be reused by a given account for a period of one year.
4. All accounts must be suspended indefinitely after 3 consecutive invalid log-in attempts. If you forget or lose your password, contact the IT help desk at extension 1499.

Mainframe Passwords
Your mainframe password consists of 8 digits and will be automatically assigned to you every 45 days.
Several days prior to the date your current password expires, you will be warned that your mainframe password will be expiring. On the 45th day, you will be assigned a new 8-digit password. It is important that you memorize this password or write it down and keep it in a safe place that is not accessible to anyone else. If you forget or lose your password, contact the help desk at extension 1499.

Password Confidentiality
Everyone must understand the need for maintaining confidentiality of passwords. The world's best password is ineffective if it has been compromised.
1. A password must be treated as JIB confidential information at a minimum.
2. Passwords must not be posted or exposed to the view of others.
3. A password must be changed immediately if there is any possibility that it was compromised. If you need help changing your password, please contact the IT help desk at extension 1499.
4. Passwords must not be written on paper or stored in a computer file unless the paper or file is stored in a place accessible only by the owner of the account(s) protected by the password.
5. Whenever possible, passwords should consist of upper and lower-case letters, numbers, and punctuation.

Employee and Member Records
JIB employees are reminded that most information about individual members and employee health records is considered confidential under federal law and may not be released to unauthorized personnel without permission from the member or employee. This includes records of an employee's network or computer activity, involvement in security incidents and similar information, as well as participant and member personal data.

Exchanging Confidential Information
Employee and member records must be protected by a level of security commensurate with their confidentiality.
Member records should not be maintained on publicly accessible systems (such as the internet), even if the public is normally allowed to access that particular data. All sensitive data provided to parties external to the JIB (benefit providers, vendors, banks, contractors, etc.) must be encrypted. Under no circumstances should unencrypted data be sent to anyone outside of the JIB. This policy applies regardless of the method used to transfer the data: floppy disk, CD-ROM, email, conventional mail, or other medium. Instructions for using the JIB's encryption software are maintained separately. External parties who send data to the JIB, either through the mail or electronically, are strongly encouraged to encrypt the data or will be required to do so in the future.

Email
Electronic mail (email) is rapidly becoming the preferred method of business communication because it is fast, inexpensive, and relatively simple to use. This innovation, however, is not flawless: Email is one of the leading conduits of viruses across computer networks through infected messages or their attachments. Email is often used to spread "hoaxes" causing undue concern and insensitivity to real future threats. Email typically makes numerous stops at computers along the route to its final destination. At each stop, it can be intercepted and read by prying eyes.
The use of email at the JIB is intended for work purposes only and cannot be used for personal use unless authorized by Management. The JIB has taken several security measures to ensure that all email coming into the company is safe and will not harm your computer, the JIB, or the JIB's work environment. However, if you suspect any type of virus or unknown program in your email, do not open the email and report it to the IT help desk at extension 1499.

Junk Email (Spam)
The email gateway which connects the JIB to the internet is equipped with a device called a spam filter to detect and delete junk email. The spam filter is effective at blocking almost all junk email. Nonetheless, a piece of junk email may occasionally find its way into your electronic in basket. Employees should be wary of suspicious-looking emails and delete any junk mail they receive without opening it. Questions about whether a specific piece of email is spam should be directed to the IT help desk at extension 1499.
If a JIB employee receives more than a few pieces of junk email per month, it may indicate that there is a problem with that user's email settings or with

the spam filter. Users who receive spam frequently should contact the IT help desk at extension 1499.

Avoiding Breaches

In accordance with the Joint Board's Privacy Policies and Security Policies the Joint Board shall take all reasonable and necessary steps to avoid Breaches. A Breach is defined as the acquisition, access, use, or disclosure of PHI or ePHI in a manner not permitted under the Privacy Rule (unless a limited exception applies, or the Joint Board determines that the PHI or ePHI was not compromised).

If a workforce member or person acting under the authority of the Joint Board believes that an event may constitute a Breach, as defined above, such individual or entity shall report the event (an "Apparent Breach") and any relevant additional information to the Joint Board's Privacy Officer and to the Joint Board's Security Officer in accordance with the Joint Board's Privacy and/or Security Policies.

Reporting Suspicious Events

Employees are asked to report suspicious or unusual events. In addition to Social Engineering, Pretexting, Email Hoaxes and Phishing Scams, such events may include (but are not limited to) unauthorized access of the network (from both internal and external sources), compromise of sensitive data, destroying hardware or software, and malicious code such as viruses, worms or any other unauthorized software. Immediate reporting of events will help mitigate any adverse impact and minimize current and future vulnerability. You should report even those events that seem trivial. To report an event immediately, contact Steve Butman, the HIPAA Security Officer, at extension 1552. Department personnel will document the report on a Suspicious or Unusual Event Form. A copy of this form can be downloaded from ttp://tesla/jib-doco/SuspiciousEventForm.pdf.

When you first notice a suspicious or unusual event, use the form to collect all relevant and important details.

Enforcement and Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. If an employee violates this policy for the first time, he or she will be given a written and verbal warning; however, depending on the nature of the violation, a first offense can be grounds for termination. If there is a second violation, the person will be suspended without pay from their job responsibilities and may be terminated based on the nature of the violation. The length of suspension will be commensurate with the severity of the incident. If this policy is violated a third time by the same individual, he or she will be terminated immediately.

The Security Policies and Procedures apply to all users of JIB information, including employees, medical staff, outside vendors and consultants. Failure to comply with information security policies by employees, medical staff, outside vendors and consultants may result in disciplinary action up to and including dismissal in accordance with applicable JIB procedures, or, in the case of outside vendors and consultants, termination of the affiliation. Further penalties associated with state and federal laws may apply. Possible disciplinary or corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of PHI, ePHI or confidential information.
2. Unauthorized disclosure of a user id, sign-on code, or password.
3. Attempting to obtain a user id, sign-on code, or password that belongs to another person.
4. Using or attempting to use another person's user id, sign-on code, or password.
5. Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.
6. Installing or using unlicensed software on JIB computers or laptops.
7. The intentional unauthorized destruction of JIB information.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.
9. Failure to lock a computer when leaving the workstation.
10. Use of a cell phone camera to photograph protected information (such as a picture of the computer screen, reports, medical claims, correspondence, etc.).

Some Examples of PHI

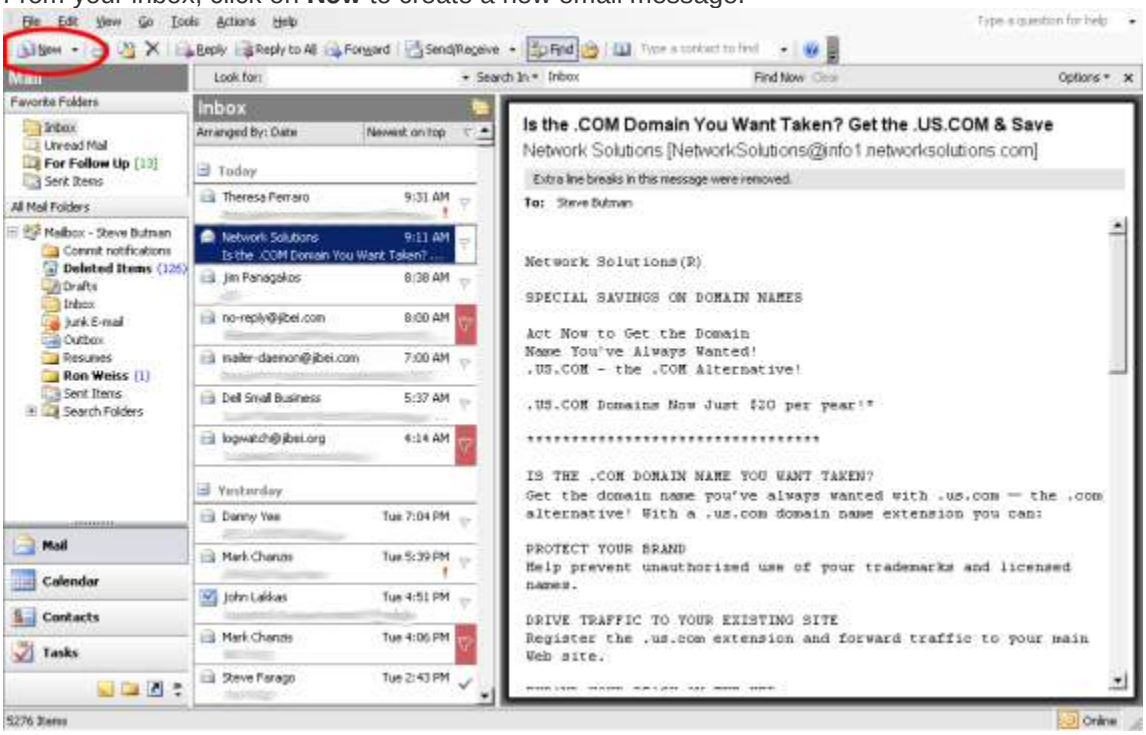
PHI is health information that meets all of the following criteria:

- Information a Health Plan creates or receives about an individual
- Information relating to the individual's past, present or future health condition or past, present or future payment for health care services
- Information that either identifies the individual ("individually identifiable health information") or creates a basis upon which a disclosing entity should believe that the information is used to identify an individual.
- Individual identifiers include: Name, SS#, telephone number, fax numbers, e-mail address, full-face photographic image or other conditions that identify an individual or a group of individuals.

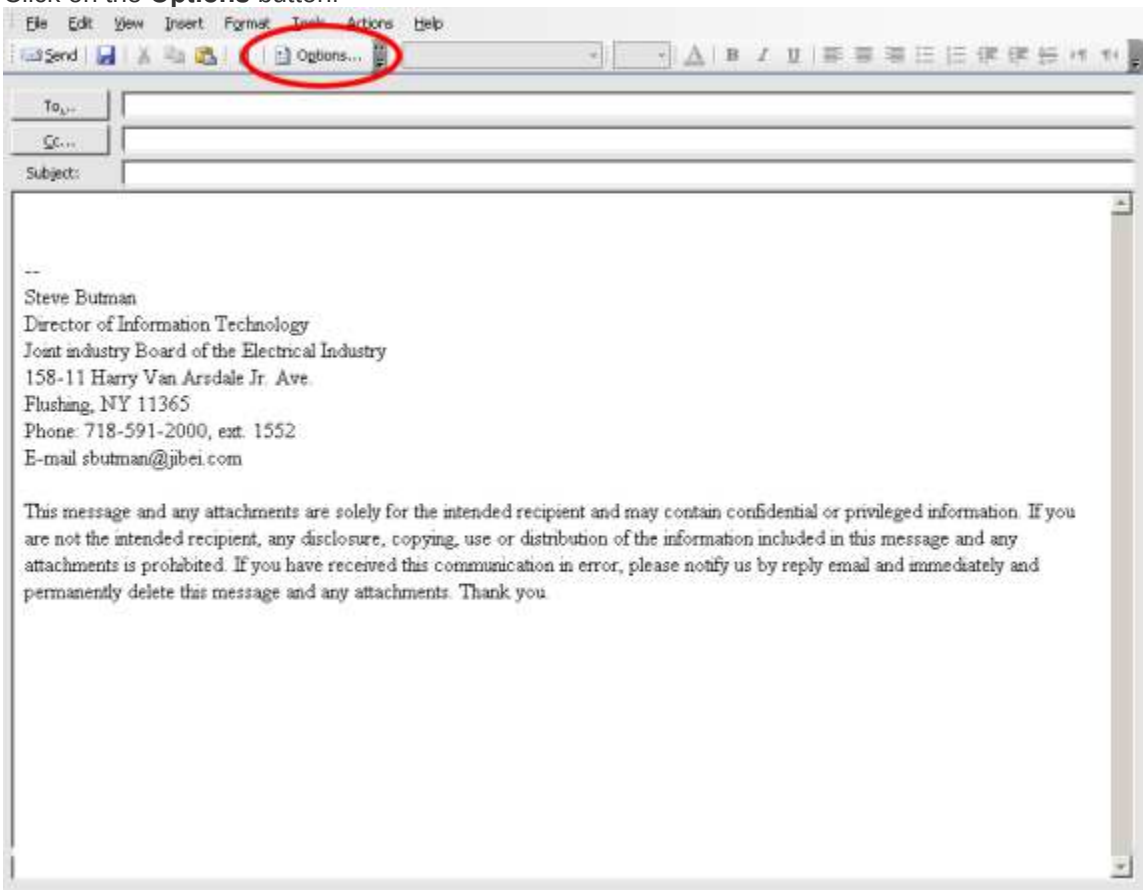
Sending an Encrypted Email

In order to maintain the privacy of our members and employees, it is often necessary to secure confidential information such as social security numbers, financial data, or even home addresses. The JIB security policy forbids sending sensitive information outside of the JIB unless such information is encrypted and cannot be read by unauthorized parties. Fortunately, sending confidential information in a secure fashion is very easy.

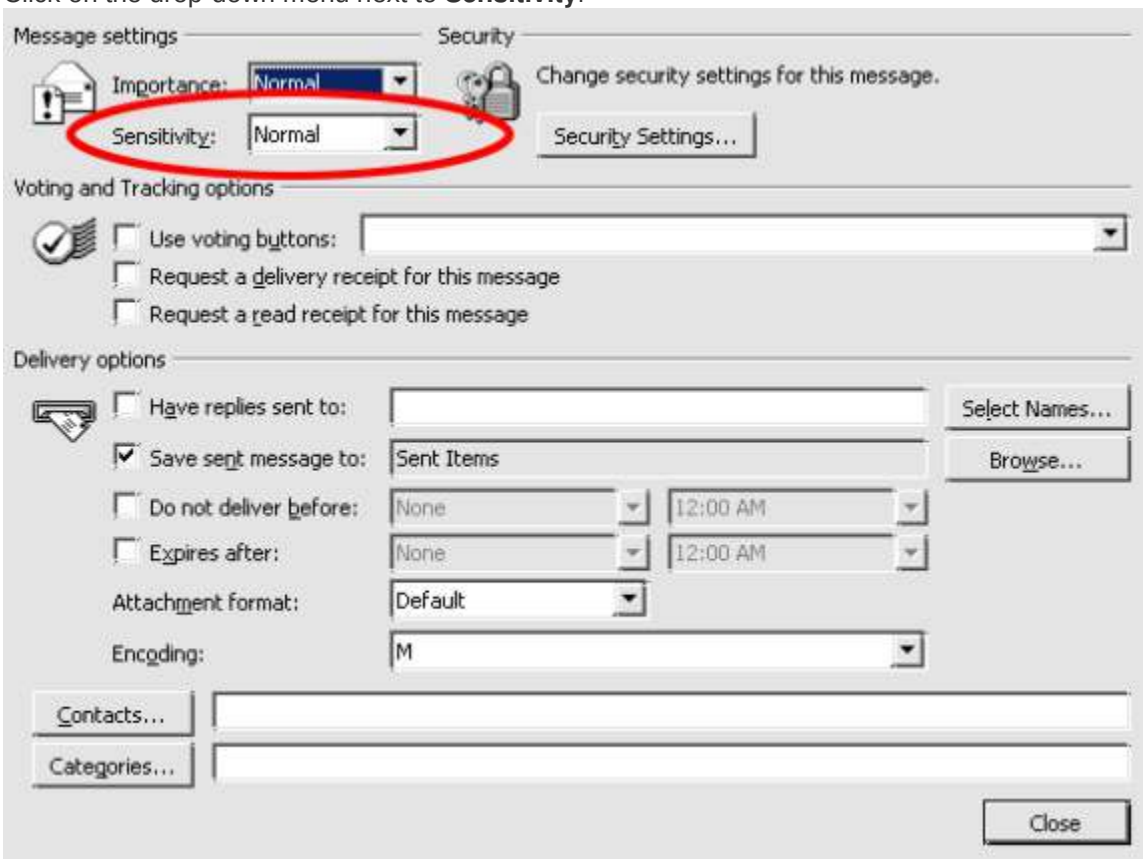
1. From your inbox, click on **New** to create a new email message.



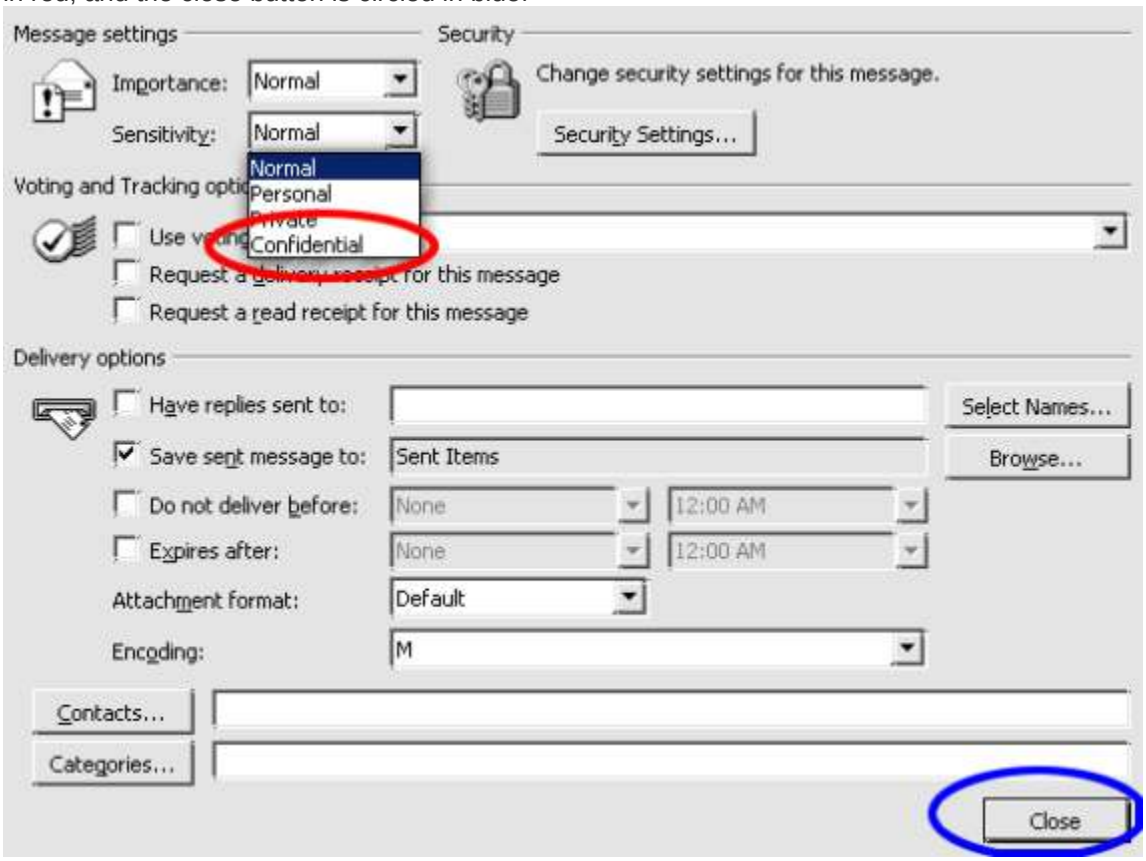
2. Click on the **Options** button.



3. Click on the drop-down menu next to **Sensitivity**.`

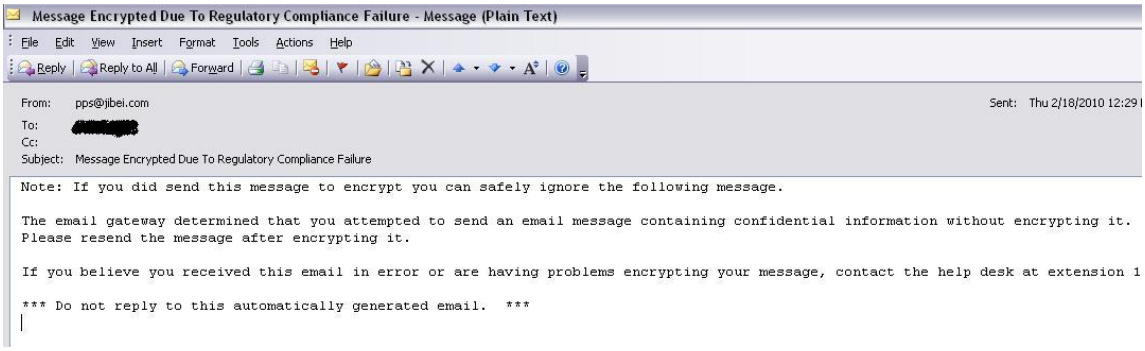


4. Select **Confidential** and close the window. In the screenshot below, the confidential setting is circled in red, and the close button is circled in blue.



5. Finish typing your email, adding attachments as necessary, and send it the way you normally would.

Our software checks in both the title and the body of your email for any confidential information which is not supposed to be sent external to the company. If some confidential information is sent out, you will receive a notification from the software as the screen shows below.



That's all there is to it. Your email will now be encrypted and secured from reading by unauthorized parties. The recipients of the email will automatically receive instructions about how to open it.

By signing this form, I acknowledge that I have read the Joint Industry Board of the Electrical Industry HIPAA Privacy and Security Training Manual and agree to adhere to and abide by the HIPAA Privacy and Security Policies and Procedures adopted by the Joint Industry Board.

_____

Name *(please print)*

_____

Signature

_____

Department

_____

Date