PURPOSE
To establish a policy respecting the access, use, disclosure, and safeguarding of protected health information (PHI) received by The Joint Commission.

POLICY
In order to carry out its mission to improve the safety and quality of health care through accreditation and related services, healthcare organization customers may provide The Joint Commission access to PHI. Where contracted work performed on behalf of a healthcare organization requires access or use of PHI, The Joint Commission Enterprise will ensure that a business associate or other relevant HIPAA agreement is in place. This Joint Commission policy provides for the safeguarding of that PHI to afford it the utmost privacy and confidentiality as required under the HIPAA Privacy and Security Regulations. In the case of PHI received for research purposes, the Research Policies will be followed.

Access to Information – To ensure that PHI is protected from improper or unauthorized access, use, or disclosure, Joint Commission employees and other authorized individuals shall access only the information necessary for the business purposes for which they are responsible, in accordance with the relevant contracts and Joint Commission policies, procedures, and practices.

Joint Commission employees and other authorized individuals are to access or use PHI only when necessary to carry out their duties and responsibilities on behalf of The Joint Commission. Access to PHI for research purposes shall not be provided until the information has been de-identified, or patient authorization has been obtained, or the PHI has been received from a health care organization under a research contract or a data use agreement, and/or its use has been authorized by an Investigational Review Board when required. (See Research HIPAA policies.)

Safeguarding Information – Joint Commission employees and other authorized individuals who possess or control PHI shall safeguard this information to prevent its unauthorized disclosure and protect it from inappropriate release. (See also the Enterprise Data Security Strategy and Standard policy).

Minimum Necessary Information – The Joint Commission shall access and use only the PHI necessary to fulfill its responsibilities. In order to satisfy a minimally necessary standard, The Joint Commission shall:
JOINT COMMISSION
CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

Section: Privacy and Security
Effective: September 2006
Applies to: All Joint Commission Enterprise Staff

- Obtain information in a de-identified format, whenever possible, to avoid use of PHI unless absolutely necessary.
- Authorize only those individuals whose roles make it necessary for them to access PHI to do so.
- Use information obtained in accordance with this policy only for the purpose for which it was obtained.

Disclosure of PHI – The Joint Commission is to disclose PHI only in accordance with the purpose for which it was obtained to the organization or individual that supplied the information and/or as follows:
- When required by law and authorized by the Joint Commission Legal Department; or
- When used by an authorized contractor under a written Business Associate-Subcontractor agreement which specifies that the information shall be held confidentially and used only as authorized.
- When used under a research agreement or data use agreements in accordance with the described research.

Storage and Disposal of PHI – PHI in the possession of The Joint Commission, its employees, and/or agents shall be stored in a secure manner. When PHI is no longer needed for the purpose for which it was collected, it shall be de-identified, returned to the source, and/or disposed of in a secure manner.

DEFINITIONS

Authorized Individuals – Employees, volunteers, trainees, Commissioners, and contractors who are authorized to access or work with PHI, because they have received training and because of the functions they perform for The Joint Commission.

De-Identified - Data will be considered de-identified only if the data has been certified as de-identified or all of the following elements have been removed:
- Names;
- All geographic subdivisions smaller than a state;
- All dates directly related to the individual, ages over 89;
- Telephone numbers;
- Fax numbers;
• E-mail addresses;
• Social security numbers;
• Medical record numbers;
• Health plan beneficiary numbers;
• Account numbers;
• Certificate/license numbers;
• Vehicle identifiers and serial numbers;
• Device identifiers and serial numbers;
• Web URL’s;
• IP addresses;
• Biometric identifiers;
• Full face photos; and
• Any other unique identifiers.

Where appropriate, employs an authorized statistician to certify that a database is de-identified.

Disclosure – The release, transfer, provision of access to, or the divulgence in any manner (written, oral, or electronic) of protected health information.

Protected Health Information (PHI) – Information created by and/or received from a health care provider, health plan, or health care clearinghouse that identifies an individual for which there is reasonable basis to believe that it could be used to identify the individual, and that relates to:
• The past, present, or future physical or mental health or condition of an individual; and/or
• The provision of health care to the individual; and/or
• The past, present, or future payment for the provision of health care.

Research – A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
Use – the sharing, employment, application, utilization, examination, or analysis of such information by the Joint Commission employees and other authorized individuals.

References
HIPAA Privacy and Security Rules 45 CFR Section 164 where relevant to business associates.

PROCEDURES

ACCESS

Employees/Authorized Individuals

1. Upon hire or change in position within the organization, each employee and authorized individual shall be authorized by policy or management to access paper or electronic files containing PHI, and to the areas or computer systems where the files are housed. HR initiates the Information Systems authorization process by submitting a request to the Department Head or manager, if their role requires such access. The request should include documentation of the business rationale for their authorization to access PHI.

2. After receiving authorization, access only that PHI necessary to carry out the duties and responsibilities on behalf of The Joint Commission.

Principle Research Project Investigators (PI)

3. The PI is responsible for safeguarding the PHI from unauthorized access consistent with Research policies.

Department Head

4. The Department Head has overall responsibility for review and approval of requests for access to PHI within the department, and for employees or authorized individuals outside the department and will allow access to records containing PHI only after the requestor demonstrates appropriate authorization from his/her Department Head.

   a. Department Head shall ensure records containing PHI are archived in a manner consistent with the Records Retention Policy.
Information Technology
5. Reviews authorization and provides access to databases, software, and computer systems containing any PHI only to requesters who have received authorization from the appropriate authorized individual.

ADMINISTRATIVE SAFEGUARDS
Compliance Council
1. Reviews this policy and procedure regularly to determine if revisions are needed to ensure the protection of PHI.

2. Regularly reviews information provided by the Corporate Compliance and Privacy Officer and Information Security Officer, including audits, access reports, and security incident tracking.

Department Head
3. Ensures that all hard copy PHI that is retained within the Department is secure, and that access and use of ePHI is consistent with the privacy and security policies.

4. Ensures that employees or authorized individuals who work remotely are educated on this policy to keep PHI secure.

5. Ensures that all employees and authorized individuals within the Department are appropriately authorized prior to access and use of PHI.

6. Ensures that when an employee is terminated appropriate termination procedures are followed to remove access to PHI immediately.

7. Also ensures and encourages all department personnel to follow security procedures and report all privacy and security incidents.

6. When contracted work requires access to PHI, to ensure that either a Joint Commission template contract is used or the contract is handled consistent with the defined contract routing process.

Security Officer/IT
8. Completes a security risk assessment, analysis, and management plan on a regular basis and present to the Compliance Council.

9. Creates and administers a Business Continuity Management Plan that includes regular testing and a provision to update.
Human Resources

10. In conjunction with management will sanction employees or other Authorized individuals for any privacy or security infraction consistent with appropriate disciplinary procedures.

Corporate Compliance and Privacy and Information Security Officers

11. Ensure that privacy and security training are provided on those policies that relate to access, use, and disclosure of PHI. Training shall include:

- Providing policy training to employees and other authorized individuals with a refresher on reporting of infractions on an annual basis; and

- Coordinating a review of policy and training for inclusion in Orientation.

- Security Awareness updates.

12. Provide reports to the Compliance Council regarding privacy breach, security incidents, and coordinate the handling for both.

Legal Department

13. Legal staff will ensure that when the contract review and due diligence process identify access or use of PHI in the course of the business relationship, a business associate agreement or other HIPAA appropriate agreement will be incorporated into the contract.

PHYSICAL SAFEGUARDS

Each Employee/Authorized Individual

1. Ensures that any documentation containing PHI is kept out of the sight of individuals who have no business need to know.

2. Is responsible for protecting confidential information that includes PHI when he/she has visitors.

3. When copying or transmitting PHI via fax machine, supervises usage of the fax machine or copier.
4. Verify that individuals requesting access to information containing PHI have appropriate authorization before they are allowed access.

5. Provide access to documents only as outlined in the requestor’s authorization.
Managers of Areas Accessing or Using PHI

6. Develop internal procedures safeguarding paper files used or stored within the department.

7. Review physical space for audio privacy to ensure that discussions with health care organizations are not disclosed to individuals other than those with a need to know. Specifically this includes:
   • Sentinel event and complaint handling discussions; and
   • Reviews of organization responses to accreditation decisions and review hearing panel documents.

8. Review personal computers and workstations to determine need for technical security aids.

9. Implement procedures ensuring that desks are clean when unattended and file cabinets containing PHI are supervised or locked.

10. Ensure that appropriate containers and/or shredders are available at convenient locations and used for staff to dispose of any unarchived documents containing PHI.

TECHNICAL SAFEGUARDS

Information Technology

1. Monitors access to databases and systems containing PHI and reports to the Compliance Council.

Employees/Authorized Individuals

2. Comply with the Security Policies for access to any systems containing PHI.

Director of Technical Services, Security and Compliance

3. Reviews and maintains the Security Policies to ensure standard applied is relevant and accurate to protect the integrity and transmission security of PHI.
MINIMUM NECESSARY INFORMATION

Managers
1. Evaluate the need for employees or other authorized individuals to have access to PHI, based on job descriptions, and ensure that access is limited to what is necessary to properly complete Joint Commission duties and responsibilities.

2. Review department processes to evaluate where de-identification might be appropriate and whether the access to PHI received from healthcare organization customers may be minimized.

Information Technology
3. Ensures that, except for access by approved employees and other authorized individuals, only de-identified health data is accessible.

DISCLOSURE OF PHI

Employees/Authorized Individuals
1. Disclose PHI only as follows:
   a. To the organization or individual that supplied the information.
   b. According to policy authorized by the Legal Department, or the Corporate Compliance and Security Officers.
   c. To an authorized contractor with a current Business Associate-Subcontractor agreement in place.
   d. As outlined in the research and data use agreements and in accordance with the purpose for which it was obtained.

Authorized Contractors
2. Contracts for any companies or individuals authorized to access, use PHI will include the following:
   a. Notify the Corporate Compliance and Privacy Officer of any known instances of unauthorized disclosure of PHI. Any intentional violation of this policy will be grounds for contract termination.
   b. Notify the Security Officer for any security breach.
STORAGE AND DISPOSAL OF PHI
Employees/Authorized Individuals
1. Designated all hard copy files with for the archive files as Confidential, and ensure it is archived in a secure location. The preferable method of archiving is electronic.

2. If hard copy PHI is no longer needed for the purpose for which it was collected, it can only be disposed of consistent with the records retention schedule by de-identification, it can be returned to the source, and/or disposed by shredding.

3. ePHI shall be retained consistent with the records retention schedule and in a space that meets the HIPAA security requirements.

COMPLIANCE
Compliance Council
1. Ensures that appropriate audits and monitors are in place, and that reports are completed regularly, consistent with the audit schedule. These audits and monitors are to address the administrative, physical, and technical safeguards protecting PHI.

2. Working with the Privacy and Security Officers, determine the need for risk assessment.

3. Conduct a review to ensure that contracts are in place for all contractors to whom the Joint Commission provides PHI.

President, General Counsel, Security, and Privacy Officers
4. During any material breach in privacy or security:
   - Follow the Critical Incident Response Plan and/or the Reporting an Information Privacy or Security Incident policies when determining the steps necessary to mitigate, to the extent practicable, any potential harmful effect of the breach; and
   - When indicated Report to the affected organization the nature and consequences of the breach.

5. Provide review and approval when the Secretary of the Department of Health and Human Services (HHS) requests access to the Joint Commission Enterprise Staff.
Commission’s internal practices, documentation, policies and procedures, books, and records relating to the use and disclosure of PHI for purposes of determining compliance with the Privacy and Security Rules.
Officer with Divisional Responsibility, Security and Privacy Officers

6. Ensure that procedures are in place to account for disclosures of PHI as required by law.

7. Review all requests from unauthorized organizations or individuals for any of the following:
   • An accounting of disclosures;
   • Access to PHI;
   • Incorporating amendments or corrections into PHI.

ORIENTATION TRAINING

Human Resources and Managers

1. Ensure that, at orientation, each new hire and Board member receives:
   • Information about the Privacy and Security Policies; and
   • Compliance training coordinated by the Privacy and/or Security Officers, or their designees, which includes reporting requirements.

2. Ensure that all trainees, interns, students, observers, volunteers, or contractors working in areas that contain or use PHI complete training when they begin working for The Joint Commission.

3. Handle intentional unauthorized disclosures consistent with disciplinary policies or as a breach of contract for authorized contractors.

APPROVALS

Policy Approval – This policy statement requires the approval of the President of The Joint Commission.

Procedure Approval – The initial procedure and any changes thereto require the approval of the Compliance Council.

Reviewed and updated December 2013, and July 2016