HIPAA REFERENCE GUIDE

1. **What is HIPAA?** Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - Gives patients more control over their health information
    - Sets boundaries on the use and disclosure of health information
    - Establishes appropriate safeguards to protect the privacy of health information
    - Holds Violators accountable with civil and criminal penalties that can be imposed if they violate a member's privacy rights
2. **The Privacy Rule** establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and wellbeing. This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance.
3. **The Security Rule** specifically focuses on the safeguarding of electronic protected health information (EPHI). All covered entities under HIPAA must comply with the HIPAA Security Rule, which establishes a set of security standards for securing certain health information. **Administrative safeguards** are defined as the "administrative actions, policies, and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." **Physical safeguards** are defined as the "security measures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion." **Technical safeguards** are defined as the "technology and the policy and procedures for its use that protect electronic protected health information and control access to it." These categories of safeguards encompass the continuum of security for electronic healthcare information for covered entities under HIPAA. The security process begins with the policies and the procedures that establish personnel behavior and provides a framework for acceptable access to and uses of protected health information. These administrative controls are the foundation for the HIPAA Security Rule. The physical safeguards support limitations to restricted spaces and equipment, including materials that contain electronic protected health information. Technical safeguards apply specifically to information systems and are measures of protection associated with the actual hardware, software and networks for these systems.
4. **What is HITECH?** The Health Information Technology for Economic and Clinical Health Act Is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to healthcare information technology in general (e.g. creation of a national healthcare infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.
5. **Covered entities are defined in the HIPAA rules as:**
    - health plans
    - healthcare clearinghouses

- healthcare providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards

6. **What is Protected Health Information?**
   Protected Health Information (PHI) is individually identifiable health information held or maintained by Benefits Administration, or our business associates who act on our behalf, that is transmitted or maintained in any form or medium.
   PHI is health information:
   - Received by a provider, plan or certain other entities;
   - Relates to an individual's past, present or future physical or medical condition or healthcare or payment for healthcare; and
   - Identifies or could reasonably be used to identify an individual

7. **Electronic PHI** (ePHI) is protected health information that is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media.

8. **What information must YOU Protect?** 17 most common identifiers related to individual, relatives, employers or household members: name, health plan beneficiary number, postal address, all elements of dates except year, telephone number, email addresses, URL address, IP address, social security number, account numbers, license numbers, medical record number, device identifiers and their serial numbers, vehicle identifiers and serial number, biometric identifiers (finger and voice prints), full face photos and other comparable images and **any other unique identifying number, code, or characteristic.**

9. **Our plan members have certain rights regarding the privacy of their PHI. The Privacy Notice explains those rights and obligations to the member.**
   Plan members have a right to:
   - Access and receive a copy of their paper or electronic medical record
   - Request amendments to their health information
   - Request restriction of, or limitations on how to use and disclosure of their PHI
   - Restrict disclosure to health plans for services self-paid in full ("self-pay restriction")
   - Request confidential communication
   - Receive an accounting of the disclosures of their PHI
   - File a complaint
   - Choose someone to act on their behalf

10. **What is a "business associate"?** A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
    - Benefits Administration Business Associate Agreement (BAA) requires specified written safeguards for PHI.
    - ARRA requires Business Associates to comply with all the same regulations as Benefits Administration.
    - Benefits Administration Business Associates have the same penalties for violations as Benefits Administration.
    - Business Associate Agreement (BAA) must be included with contract.

11. **Privacy Rule is designed to protect individuals' health information and allows individuals to:**
    - Get a copy of their medical records
    - Ask for changes to their medical records
    - Find out and limit how their PHI may be used

- Know who has received their PHI
- Have communications sent to an alternate location or by an alternate means
- File complaints and participate in investigations

12. **You may disclose information without a member's authorization <u>to the appropriate authorities</u>:**
    - If required by law, court order
    - To public health officials, FDA
    - For abuse or domestic violence
    - To help law enforcement officials
    - To notify of suspicious death
    - To provide information for workers' compensation
    - To assist government actions
    - To help in disaster relief efforts
    - To avert a serious threat to health or safety
    - For health oversight activities
13. **The Minimum Necessary Standard**, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.
14. **When can you Access, Use, or Disclose ePHI?** HIPAA allows you to access, use or disclose ePHI for three purposes without consent from our member.
    - For Treatment – the provision, coordination or management of healthcare by one or more healthcare providers, including consultation between healthcare providers
    - For Payment – activities to obtain payment or reimbursement for services or premiums
    - For Healthcare Operations – administrative, financial, legal and quality assessment and improvement activities and fraud and abuse detection

    Other uses and disclosures require the patient's specific authorization (and signature) using the **<u>Release of Protected Health Information Form</u>**
15. **A valid authorization must contain at least the following elements:**
    - A specific/meaningful description of the information to be used or disclosed;
    - The name/entity who is authorized to release PHI;
    - The name/entity who is authorized to receive PHI;
    - If the authorization is signed by a personal representative legal documentation must be presented along with the authorization;
    - A description of each purpose of the use or disclosure;
    - An individual's right to revoke and how they may revoke
    - The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization;
    - A statement regarding the potential for re-disclosure by the recipient of the information;
    - The signature of the individual and the date; and
    - An expiration date or event.
16. **When a HIPAA release form is completed, does the ABC need to send that form to Benefits Administration as well as keep one on file?** If the HIPAA release form is authorizing Benefits Administration to release an employee's PHI, you should send the release to the Benefits Administration's HIPAA Privacy and Security Office at <u>benefits.privacy@tn.gov</u>. Benefits Administration will scan the authorization into Edison under the employee's record. You should retain a copy for your records.

17. **Can the HIPAA release form be open-ended?** No, there must be a specified end date or expiration event. The expiration event can state "upon my termination," "upon my death," or any other similar statement.
18. **Security Rule is designed to secure the transfer and storage of electronic health information (ePHI) by enforcing:**
    - **Administrative Safeguards:** These measures manage the selection, development, implementation and maintenance of security measures and include workforce security, security training, policies and procedures.
    - **Technical Safeguards:** The technology that protects ePHI and controls access and transmission security.
    - **Physical Safeguards:** Physical measures to protect the electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
19. **Fax Security**
    - Avoid faxing confidential information. If you send a fax to an incorrect number, report the incident immediately to your supervisor.
    - Verify fax numbers prior to transmission to ensure the fax will be going to the correct person.
    - **ALWAYS** use fax cover sheet
    - The fax cover sheet should contain a confidentiality notice requesting notification if the fax went to the wrong person.
20. **A breach** is defined as the acquisition, access, use or disclosure of unsecured PHI which is not permitted by the HIPAA Privacy Rule and which compromises the security or privacy of the PHI.
21. **Email**
    - Emails about members should only be shared with those who have a need to know this information in connection with their specific job function(s).
    - Emails sent externally should be encrypted.
    - Certain issues should never be discussed via e-mail. For example, members' HIV status, or mental health treatment, or treatment for drug or alcohol abuse, should not be discussed via e-mail due to their extremely sensitive nature and the potential risk to the member should the information be inadvertently disclosed.
    - Verify the identity of the recipient before replying.