State of Maryland
Department of Budget & Management
Employee Benefits Division

Privacy Policy

November 2017

Introduction

In accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the US Department of Health and Human Services (HHS) has established rules to protect the privacy of health information maintained by health plans, health care providers and certain other health care entities (collectively, covered entities). HHS has developed a comprehensive regulatory scheme governing the treatment of the health information that is covered by the HIPAA Privacy Rule, known as protected health information (PHI). Pursuant to the HIPAA Privacy Rule, covered entities generally must comply with the following obligations: (i) use or disclose health information only as permitted by the HIPAA Privacy Rule standards; (ii) limit requests, uses and disclosure of health information to minimum necessary; (iii) give participants a notice of the entity's privacy practices; (iv) provide participants certain rights with respect to their health information; and (v) establish certain administrative procedures to ensure health information is kept confidential. As a covered entity, the State Employee and Retiree Health and Welfare Benefits Program (the Program) is required to design and implement policies and procedures that comply with the HIPAA Privacy Rule.

The policies and procedures herein are intended to comply with the HIPAA Privacy Rule established by HHS. The Department of Budget and Management's (DBM) Employee Benefits Division (EBD) maintains such privacy policies and procedures and it is the intent of DBM EBD that these policies be interpreted consistently with the HIPAA Privacy Rule.

Definitions

Defined terms are not necessarily capitalized throughout document.

Agency Benefit Coordinators (ABC): At each participating State of Maryland agency or Satellite agency, the designated personnel who has completed HIPAA training and has been assigned by each agency to handle the administration of health benefits for its employees.

Authorization: The official grant of authority by an enrolled participant to the Program, allowing for the disclosure or use of the participant's PHI.

Business Associate: As defined in 45 C.F.R. § 160.103.

Covered Entity: As defined in 45 C.F.R. § 160.103.

Data Use Agreement: An agreement that sets out the permitted uses and disclosures of limited data sets, including who may use or receive the data and limitations on the receiving party's ability to re-identify or contact the participants who are subjects of the limited data.

DBM or Department: The Department of Budget and Management

Department of Health and Human Services (HHS): The department of the executive branch of the federal government with overall responsibility for implementing HIPAA.

Dependent – An eligible person as defined in COMAR 17.04.13.03(A)(9), as amended from time to time. *See* http://www.dsd.state.md.us/comar/getfile.aspx?file=17.04.13.03.htm.

Dependent Child(ren) – An eligible person as defined in COMAR 17.04.13.01(B)(3), as amended from time to time. *See* http://www.dsd.state.md.us/comar/getfile.aspx?file=17.04.13.01.htm.

Disclose or Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

EBD: Employee Benefits Division of the Department of Budget and Management.

Health Care: As defined in 45 C.F.R. § 160.103.

Health Care Clearinghouse: As defined in 45 C.F.R. § 160.103.

Health Care Operations: Activities related to the clinical management and administrative duties of a health care business or practice. Some examples of these activities are: use of PHI to obtain a referral; quality assurance; quality improvement; case management; training programs; licensing; credentialing; certification; accreditation; compliance programs; business management; and general administrative activities of the practice. Health Care Operations is further defined to include all activities associated with the selling, merging, transferring or consolidation of medical practices and other covered entities.

Health Care Provider: As defined in 45 C.F.R. § 160.103.

Health Information: Means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of

health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): A federal law enacted in 1996 that protects continuity of health coverage when a person changes or loses a job, that limits health plan exclusions for preexisting medical conditions, that requires that patient medical information be kept private and secure, that standardizes electronic transactions involving health information, and that permits tax deduction of health insurance premiums by the self-employed.

Health Plan: an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C.300 gg-91(a)(2)), and as defined in 45 C.F.R. § 160.103.https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec160-103.pdf

Incidental Use or Disclosure: Is defined by the Privacy Rule "as a secondary use or disclosure that cannot reasonably be prevented, that is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure." The Privacy Rule permits certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect a participant's privacy.

Individually Identifiable Health Information: means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or, with respect to which there is reasonable basis to believe the information can be used to identify the individual.

Limited Data Set: A limited data set is PHI that excludes certain identifiers but permits the use and disclosure of more identifiers than in a de-identified data set. In particular, the limited data set allows the inclusion of all dates, 5 digit ZIP codes, and city as indirect identifiers. A limited data set may be used only for the purposes of research, public health, or health care operations.

Minimum Necessary: In the context of HIPAA, this is the principle that, to the extent practical, PHI should only be disclosed to the extent needed to support the intended purpose of the disclosure of the information.

Notice of Privacy Practices: A document used to inform participants of their rights surrounding the protection of their PHI.

Participant: Person who is the subject of PHI. This includes enrolled employee, retiree, dependent (as defined by COMAR 17.04.13.03(A)(9) and dependent child(ren), as defined by COMAR 17.04.13.01(B)(3).

Payment: Encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

Personal Representative: A person who, under applicable law, has the authority to act on behalf of a participant in making decisions related to health care.

Plan Document: A written document that sets forth each plan's terms and conditions within the Program.

Program: The Maryland State Employee and Retiree Health and Welfare Benefits Program.

Plan Representative: Personnel who are employed by our covered entities or business associates, or have been granted the authority to represent such covered entities or business associates, pursuant to the terms of any contracts between the Department and the covered entities and/or business associates.

Privacy Official: The individual who has been designated as responsible for the development and implementation of a plan's privacy policies and procedures. DBM's Privacy Official is Kelly Valentine, Compliance Officer, Employee Benefits Division, 301 West Preston Street, Room 510, Baltimore, MD 21202, 410-767-4775.

Protected Health Information (PHI): Protected health information means individually identifiable health information: (1) Except as provided in section (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20

U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.

Third Party Administrator (TPA): An organization that processes insurance claims or certain aspects of employee benefit plans for a separate entity.

Treatment: The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

Use: With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within the entity that maintains such information.

Statement of Privacy Policy

EBD will protect the privacy of all affected participants' PHI in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), federal regulations promulgated pursuant to HIPAA, and applicable State laws and regulations. PHI generally will be used only for health plan administration, operations and payment requirements. It may also be used in other limited circumstances such as where required for law enforcement and public health activities. Only the minimum necessary information will be used, except in limited situations specified by law. No other uses or disclosures of PHI are permitted unless authorized by the enrolled participant. Enrolled participants may inspect, copy, and amend their PHI as allowed by HIPAA, and may exercise the rights granted to them under HIPAA free from any intimidation or retaliation.

When PHI is shared with covered entities and/or business associates that provide services to the Department, those entities will be required to agree in writing to maintain procedures that protect the PHI from improper uses and disclosures in conformance with HIPAA.

When EBD receives PHI to assist in health plan administration, operation and payment requirements, it will adhere to its own stringent procedures regarding the protection of information. Among the procedures in place are:

- Administrative and technical firewalls that limit which groups of employees are entitled to access PHI and the purpose for which they can use it;
- Rules for safeguarding PHI from improper disclosure;

- Processes to limit the disclosure of PHI to the minimum necessary;
- A verification process to identify and confirm the authority of persons requesting PHI;
- A training program for relevant staff; and
- Procedure for receiving and processing privacy complaints.

1. SAFEGUARDS

EBD has developed and implemented, and will continuously monitor and update physical, administrative and technical safeguards to reasonably protect PHI from intentional and unintentional uses or disclosure that violate the HIPAA Privacy Rule. In addition, EBD has instituted procedures to verify the identity of any person or entity requesting PHI and the authority of that person or entity to have access to PHI.

1.1 Protection Procedures

1.1.1 Physical Safeguards

Visitor and Staff Access

- EBD's office area is secured at all times by locked doors at all entrances and is accessible only by specific entry codes or the use of an ID card-swiping system. Entrance is available only to EBD employees and other approved personnel who have received HIPAA training.
- All visitors enter into the EBD office lobby and sign in with the front desk personnel. Each visitor completes a separate visitor sign-in sheet, which is given to the front desk personnel. The front lobby is secure and attended by EBD staff during business hours, and a visitor cannot enter the EBD offices unless accompanied by authorized EBD staff.
- After completing the visitor sign-in sheet, the visitor must remain in the EBD office lobby for assistance by an assigned EBD staff member.
- The assigned EBD staff member will escort the visitor to a private EBD meeting room.
- When PHI is discussed, meeting rooms are secured by closing the doors.
- After the visitor's business is complete, an EBD staff member will escort the visitor to the EBD office lobby to exit.

Documents

- Visitor sign-in sheets are maintained in secured files by the EBD Customer Service Manager.
- All enrollment forms, papers, mail, files and faxes received at EBD that contain PHI are sorted by the EBD Customer Service Manager or designee and distributed to the appropriate EBD personnel.
- At the close of the business day, all forms, reports, mail, files and faxes containing PHI are secured by the EBD unit staff member who has custody of the record.

- Each EBD Unit Supervisor is responsible for monitoring the security of forms, reports, mail, files and faxes at the close of the business day.
- Each EBD staff member must sign the Confidentiality Agreement (Attachment A) prior to working with assigned PHI.
- EBD maintains a secure filing room for all Daily Batches as described under administrative safeguards. Only designated EBD personnel who work with the daily batches have access to that filing room.
- Phone message logs completed by Customer Service Personnel are filed in secure files cabinets or offices.

1.1.2 Administrative Safeguards:

- Enrollment forms arrive daily by mail, secure email and fax, and are placed in the allocated location in the Enrollment Unit. The Enrollment staff places the forms in the proper bin within the enrollment unit for processing for the correct effective date. Blank cover sheets are placed on the top of each bin so that PHI is protected from plain view.
- Each day all work that was completed within the Benefit Administration System (BAS) and Workday (the statewide personnel information system) is filed by category – Central Employees, University Employees, Satellite, Retirees, and Direct Pay. Each batch contains the work completed each day by each staff member (the Daily Batch).

Telephone and Facsimile Communications

- Customer Service staff maintains a daily log of social security numbers, names, contact information, and reason for calls taken during the workday. These logs are retained by each staff person at his/her workstation for record keeping purposes and within the secured EBD office.
- When answering telephone calls, EBD personnel are trained to verify the identity of the participant or personal representative before any discussion begins. If it is determined that the individual calling is not a participant or personal representative, the EBD personnel will inform the caller that a written HIPAA Authorization is required in order for EBD to provide assistance to the caller. EBD personnel will require all Agency Benefit Coordinators and Plan Representatives to identify themselves and the agency/plan they represent before discussing participant information that may include PHI.
- Faxed documents from any EBD fax machine within EBD are routinely gathered, assembled, initialed, dated, and sorted by the assigned EBD personnel and distributed appropriately to EBD staff members.
- All EBD staff are responsible for faxing their own work, including collecting the fax receipt to confirm transmission. Documents faxed by EBD personnel are retained by each individual at

his/her workstation for record keeping purpose or batched appropriately within the EBD daily filing system.

Mail/Deliveries

- Mail received from the United States Postal Service (USPS) is managed by the Department of General Services (DGS) central mailroom for the entire building where DBM-EBD is located.
- Incoming USPS mail will be retrieved twice daily by cart from DGS's central mailroom by the individual responsible for receipt of mail. The incoming mail is delivered to the EBD front desk for processing by EBD front desk personnel.
- Outgoing USPS mail is delivered twice daily to the central mailroom managed by assigned DGS personnel. Mail that contains PHI is sealed by EBD personnel prior to it being picked up for processing. Mail that does not contain PHI may be delivered to the DGS mailroom unsealed; DGS mailroom personnel is responsible for securing unsealed outgoing mail at the time postage is applied.
- For incoming non-USPS (*e.g.,* FedEx, UPS) delivery services, deliveries are made directly by the service personnel to the EBD personnel working at the front desk of EBD offices. The front desk personnel will date-stamp each incoming item and deliver it to the appropriate EBD unit.
- Outgoing non-USPS packages are picked up directly from the front desk personnel. Each outgoing item that contains PHI is sealed by EBD personnel prior to it being picked up.

Correspondence

- For each incoming written correspondence, a Customer Service staff member will be designated to perform the following: review the correspondence, generate the necessary research, complete an assignment sheet to create a case file, assign a case file number and log this information into the case file tracking sheet. The case file is then delivered to the Department or EBD personnel responsible for preparing a response. Closed correspondence cases are stored in filing cabinets within the secure EBD office.
- All papers with PHI that are to be purged are placed in locked shred bins in the EBD office, and the contents are disposed of bi-weekly by the contracted professional shredding vendor.

1.1.3 Technical Safeguards

DBM follows the Department of Information Technology's (DoIT) State of Maryland Information Security Policy, which includes the Firewall and Remote Access polices. DBM and DoIT have entered into a Memorandum of Understanding (MOU) that provides the framework for DBM to receive information technology and telecommunications support from DoIT.

The State of Maryland Information Security Policy and the MOU are Attachments B and C hereto.

Within EBD, all computers and email accounts are password-protected. Passwords must be changed every 90 days pursuant to the requirements in the State of Maryland Information Security Policy. Email login is password-protected and is updated when the user password is changed. Workday and EBD's BAS is also password-protected and EBD staff is given security rights and access to information in the BAS only as required by their specific duties.

Personnel within an agency supported by the Program who are responsible for the administration of health benefits, have completed the Application and Authorization for OPSB System Access (Attachment D) and have been approved by OPSB may be granted "view only" access to the online version of the BAS. Approved personnel only have access to the records of those active employees within their assigned agency who are enrolled in benefits. Only EBD personnel and designated DoIT personnel have access to the records of all employees, retirees, direct pay members, and terminated participants, including current records and related history. The scope of access is limited by each staff member's specific position duties. Documents stored in the memory units of all copiers within EBD are erased monthly.

1.2 Verification Procedures

Prior to making a disclosure or processing a member request permitted by these Policies, unless otherwise stated in the policy, EBD Personnel must: (i) verify the identity of the person requesting PHI and the authority of such person to have access to PHI, if the identity or authority of such person is not known to EBD Personnel; and (ii) obtain any documentation, statements, or representations, whether verbal or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the disclosure or processing.

To verify identity, EBD Personnel may rely on:

a. Photo identification, written authorization, Power of Attorney or other legal document, marriage certificate, birth certificate, enrollment information, identifying number, and/or claim number;

b. If requested by health plans, providers, and other covered entities, identifying information about the entity and the purpose of the request, including the identity of a person, place of business, address, phone number, and/or fax number known to the Covered Entity;
c. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope, and de-identified information cannot reasonably be provided;
d. A request by an authorized public official upon presentation of his/her badge, identification card or other official credentials (if the request is in person) or the appropriate letterhead (if the request is made in writing). Identity also may be verified by written statement, warrant, subpoena, order, or other legal process; and
e. Personal judgement, in the rare instance where a disclosure is being made only to avert a serious threat to health or safety, or when a participant is required to be given an opportunity to agree or object to the disclosure.

2. USES AND DISCLOSURES

This section summarizes the restrictions that are imposed by the HIPAA Privacy Rule on EBD's use and disclosure of PHI and describes procedures EBD maintains to satisfy the privacy standards when it uses PHI during benefits administration. In general, a participant's PHI can be used or disclosed for a variety of administrative activities. Common examples include resolving appeals, paying claims and helping participants address coverage issues. The HIPAA Privacy Rule does not prohibit these activities, but it imposes the guidelines addressed below.

EBD must disclose PHI in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to their PHI or an accounting of disclosures of their PHI; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

EBD must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.

Consistent with the HIPAA Privacy Rule, EBD is prohibited from using or disclosing PHI that is genetic information for underwriting purposes, and may not sell PHI.

De-identified Information

The restrictions on use and disclosure apply only to health information that is individually identifiable. If the health information is de-identified, the information that can be used to identify

the individual (such as name, address or portions thereof, date of birth or other identifying dates, social security number or other identifying numbers, telephone number) has been eliminated, and the health information ceases to meet the definition of PHI and is not subject to the HIPAA restrictions regarding use and disclosure. In addition, information that has most of its identifiers removed may be disclosed pursuant to an executed Data Use Agreement.

2.1 Uses and Disclosures not requiring HIPAA authorization

EBD generally has the right to use and disclose PHI to administer the Program without obtaining authorization from the participant. For example, EBD may use and disclose PHI without authorization in the following circumstances:

- For enrollment activities and (where only summary health information is used for premium bids and plan amendment/termination activities);
- If requested by a health care provider for treatment;
- If needed for payment activities such as claims, appeals, and bill collection;
- If needed for health care administration operations, such as audits, customer service, and wellness and risk assessment programs;
- To report unlawful or unprofessional conduct or conduct that endangers others that a whistleblower believes in good faith the State has engaged in, so long as the disclosure is to a Heath Oversight Agency/ Public Health Authority or Health Care accreditation organization that has authority to investigate such conduct or to an attorney retained to advise the reporting party on legal options;
- Where a workforce member who is a victim of a crime has made a disclosure about the suspected perpetrator of the criminal act.

In some cases, EBD will want to use or disclose PHI for other purposes, in which case Authorization will be required.

Use or disclosure and the "Minimum Necessary" standard

Generally, EBD must limit uses and disclosures of PHI to the minimum degree that is necessary to accomplish the intended purpose. However, this requirement *does not* apply to:

- Disclosures to or requested by a health care provider for treatment;
- Disclosures to the participant or his/her legal representative;
- Disclosures made to the Secretary of the HHS for compliance and enforcement of the privacy;
- Uses and disclosures required by law; and
- Uses and disclosures required for compliance with HIPAA standardized transactions.

2.2 Enrollment and Disenrollment Activities

EBD will process participants' enrollment and disenrollment elections and transmit the elections to health care providers and to its business associates. Health care providers and business associates will, without obtaining a participant's authorization, disclose enrollment and disenrollment information containing PHI to EBD or its agents in the following circumstances: enrollment and disenrollment activities, including processing of annual enrollment elections; new-hire elections; enrollment changes; and responding to participant questions related to eligibility for enrollment.

2.3 Health Care Operations

The HIPAA Privacy Rule permits EBD to receive PHI other than enrollment information from covered entities including health plans, health care clearinghouses, health care providers, business associates, etc., without participant authorization, for the purpose of health care operations, which includes administrative, financial, legal and quality improvement activities that are necessary to run its business and support treatment and payment functions.

EBD has certified that it will limit uses and disclosures of PHI to Plan administrative activities and will otherwise protect PHI as required by the law. The Plan's Certification, as amended from time to time, is available from EBD by request. In general, EBD will:

- Identify the classes of employees with access to PHI and the categories of information they will use;
- Make reasonable efforts to limit disclosures of and requests for PHI to the minimum necessary to accomplish the intended purpose;
- Maintain procedures governing the storage of PHI; and
- If feasible, return or destroy PHI received from the Plan, and maintain procedures governing the retention and destruction of PHI not returned or destroyed.

3. TRAINING & COMMUNICATION

3.1 Training

EBD has created a HIPAA training program that must be completed on an annual basis by EBD employees, Agency Benefits Coordinators, and other personnel who work with PHI associated with EBD. This training is provided during its monthly ABC training meetings, during its Annual Open Enrollment training meetings, and on an as needed basis.

Sign-in sheets are maintained by the Assistant Director of EBD or an assigned designee.

3.2 Communication

EBD provides all eligible employees/retirees under the program with the written Privacy Policy in our annual "Guide to Your Health Benefits." This Guide is also provided to each new hire during onboarding.

4. INCIDENT PROCEDURES

EBD requires all of its covered entities to report to the State within five days of acquiring knowledge of: (i) any use or disclosure of protected health information not provided for by Agreement, including breaches of unsecured protected health information as required at 45 CFR § 164.410; and (ii) any security incident. EBD has incorporated into its contracts and Business Associate Agreements the appropriate processes, procedures, security practices and acceptable use policies for covered entities to utilize for purposes of identifying, responding to and managing information security incidents.

EBD is guided by DoIt's Maryland Cybersecurity Incident Response Policy, as warranted. (Attachment E)

5. CONTINGENCY PLAN

EBD is guided by DoIt's State of Maryland Information Technology (IT) Disaster Recovery Guidelines, as warranted. (Attachment F)

6. EVALUATION PROCESS

EBD continually monitors changes made to HIPAA by the HHS. This policy is reviewed at least annually to ensure full compliance with all State and federal laws and regulations.