Confidentiality and Security of Information Policy

Effective March 1, 2013
Table of Contents

Definitions

Section 1: Intent and Scope of Policy
  1.1. EGID Commitment to Privacy and Confidentiality
  1.2. The Confidentiality and Security of Information Policy and Scope
  1.3. Policy Revisions

Section 2: General HIPAA and Privacy Rules
  2.1. Requirements for a Covered Entity with Multiple Covered and Non-Covered Functions
  2.2. Protected Health Information and De-Identification
  2.3. Maintaining Confidentiality of Health Information
  2.4. Verification of Identity and Authority
  2.5. Minimum Necessary Rule
  2.6. Awareness and Training

Section 3: Uses and Disclosures of PHI
  3.1. General Rules
  3.2. Family Members and Friends
  3.3. Authorizations
  3.4. Legal, Specialized Government Functions, Workers Compensation, or Public Health Requests
  3.5. Limited Data Sets

Section 4: Participant's Rights Regarding PHI
  4.1. The Notice of Privacy Practices
  4.2. Access to Personal Health Records
  4.3. Restricting Uses and Disclosures of PHI
  4.4. Requesting a More Confidential Method of Communications
  4.5. Amendment of Records
  4.6. Filing a Privacy Complaint
  4.7. Accounting for Disclosures

Section 5: Security of ePHI
  5.1 Facility Access Controls
  5.2 Workstation Use and Security Access Controls
  5.3 User Access Control
  5.4 Audit Controls
  5.5 Device and Media Controls
  5.6 Workforce Policies for Access to Systems with PHI
  5.7 Disaster Recovery / Contingency Planning
  5.8 Data Transmission Security
  5.9 Risk Assessments: Security Management Process
  5.10 Periodic Security Evaluations
5.11 Security Incident Responses, Reporting and Mitigation
5.12 Protecting ePHI From Improper Alteration or Destruction
5.13 Evaluating, Selecting, and Implementing Authentication Mechanisms

Section 6: HIPAA Violations
6.1. Requirement to Report Violations to Privacy or Security Officer
6.2. Risk Assessment of Breach
6.3. Required Individual Notifications for Privacy Breaches
6.4. Notification to the media
6.5. Notification to the Secretary of HHS
6.6. Notification by a Business Associate
6.7. Law enforcement delay
6.8. Burden of Proof
6.9. Disclosures by whistleblowers
6.10. Disclosures by workforce members who are victims of a crime
6.11. Sanctions
6.12. Mitigation
6.13. Refraining from Intimidating or Retaliatory Acts

Section 7: Business Associates
7.1. Safeguarding PHI
7.2. Uses of PHI by the Business Associate
7.3. Access to PHI by Business Associate Employees
7.4. Safeguarding PHI by Agents or Subcontractors
7.5. Disclosure for Employment Related Actions
7.6. Notification of Breach
7.7. Access by Participants and Amendment of Records
7.8. Availability of Policies and Records to Authorities
7.9. Accounting for Disclosures of PHI
7.10. Disposal of PHI

Section 8: Participating Entities
8.1. Status of Participating Entities
8.2. Status of OMES as an Employer

Section 9: Other Privacy/Security Policies
9.1. Appointment of a Privacy Officer
9.2. Appointment of a Security Officer
9.3. Fund Raising
9.4. Storing, Access, and Destruction of Confidential Records
Definitions

**Business Associate.** As defined under the Privacy Rule, including, but not limited to, 45 CFR §160.103.

**CFR.** Code of Federal Regulations.

**Confidential Information.** Protected health information, employee personal information, member files, and other EGID information deemed confidential by EGID’s Administrator that is communicated and/or stored in any manner, including verbally, fax or other telecommunication means, on paper, or in any other electronic form. [74 O.S. § 1322]

**Covered Entity.** Under HIPAA, a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

**Covered Function.** Functions that make an entity a health plan, a health care provider, or a health care clearinghouse, as described under 45 CFR §164.103.

**De-identified Health Information.** Health information which has had all 18 HIPAA identifiers removed.

**Designated Record Set.** A group of records maintained by or for EGID that includes: the enrollment, payment, medical management, and claims adjudication record of an individual maintained by or for EGID; or other PHI used, in whole or in part, by or for EGID to make coverage decisions concerning a Participant.

**Enforcement Rule.** 45 CFR § 160 subsections C-E governing the compliance responsibilities of covered entities with respect to the HIPAA enforcement process.

**ePHI.** PHI in electronic form.

**Health Information.** Any information, whether oral or recorded in any form or medium: (1) that relates to the past, present or future physical or mental condition of a member; the provision of health care to a member; or the past, present or future payment for the provision of health care to a member; and (2) that identifies the member or with respect to which there is a reasonable basis to believe the information can be used to identify the member.

**HIPAA.** The Health Insurance Portability and Accountability Act of 1996, as amended.

**Hybrid Entity.** Under the Privacy Rule, an entity that has some covered and some non-covered functions as described under 45 CFR Section 164.103.

**Limited Data Set.** Data sets stripped of certain direct identifiers that are specified in the Privacy Rule. They are not De-identified Health Information under the Privacy Rule.

**Participant.** An individual participating in any plan authorized by or through the Oklahoma Employees Insurance and Benefits Act

**Participating Entity.** Any employer or organization whose employees or members are eligible to be Participants in any plan authorized by or through the Oklahoma Employees Insurance and Benefits Act.
**Privacy Officer.** The individual designated by EGID with responsibility for the overall implementation and oversight of EGID’s *Confidentiality and Security of Information Policy.*

**Privacy Rule.** 45 CFR § 160, Subsections A and E of §164 and associated subregulatory guidance that implement HIPAA.

**PHI.** Protected Health information, as specified in the Privacy Rule.

**Re-identified Health Information.** A code or other means of record identification to allow De-identified Health Information to be re-identified by the Covered Entity.

**Security Officer.** The individual designated by EGID with responsibility for the overall implementation and oversight of EGID’s efforts to prevent, detect, contain, and correct security violations.

**Security Rule.** 45 CFR §160 and subsections A and C of §164 that apply only to ePHI, requiring covered entities to implement certain administrative, physical and technical safeguards to protect the electronic information.

---

**Policy History**

| Effective Date of Policy: March 1, 2013 | Date Policy Last Reviewed: January 28, 2013 |
| Next Scheduled Review: December 2013 | Date Policy Last Revised: January 28, 2013 |
| Approved by: OIEBB | Prior Policy: December 2, 2011 (OSEEGIB #102) |
| | Approval Date: February 22, 2013 |
Section 1: Intent and Scope of Policy

1.1. EGID Commitment to Privacy and Confidentiality

EGID is committed to ensuring the safe handling and protection of the Confidential Information provided to EGID by its members, employees, and contractors. Confidentiality of personal records and information is taken very seriously by EGID, and strict measures will be taken to safeguard that information.

Although the Privacy Rule is applicable to health plan benefits, EGID is subject to a more encompassing confidentiality requirement under 74 O.S. §1322. Therefore, all data maintained in EGID records shall be protected in accordance with the Confidentiality and Security of Information Policy.

1.2. The Confidentiality and Security of Information Policy and Scope

The Confidentiality and Security of Information Policy establishes a framework within which EGID complies with state and federal requirements to achieve confidentiality and security of EGID Confidential Information.

All persons involved with the creation, collection, handling, and/or dissemination of EGID Confidential Information are subject to the conditions of this policy. This includes all employees, temporary workers, Insurance/Benefit Coordinators, Board Members, Business Associates, contractors and anyone who may access or view EGID Confidential Information.

1.3. Policy Revisions

This policy shall be reviewed annually, or whenever statutory or regulatory changes affecting Confidential Information occur.

EGID will maintain revised policies and procedures in written or electronic form according to Oklahoma law for at least six years from the date last in effect.

Whenever there is a change in federal or state law or regulation that necessitates a change to the Confidentiality and Security of Information Policy, the Confidentiality and Security of Information Policy is deemed revised to comply with the required change.

Policy History

| Effective Date of Policy: March 1, 2013 | Date Policy Last Reviewed: January 28, 2013 |
| Next Scheduled Review: December 2013 | Date Policy Last Revised: January 28, 2013 |
| Approved by: | Prior Policy: December 2, 2011 (OSEEGIB #102) |
| | Approval Date: February 22, 2013 |
Section 2: General HIPAA and Privacy Rules

2.1. Requirements for a Covered Entity with Multiple Covered and Non-Covered Functions

OMES includes both covered and non-covered components and has declared itself a HIPAA Hybrid Entity under the terms of 45 CFR § 164.103. EGID’s health insurance program is specifically identified as a covered component of OMES performing functions covered by HIPAA.

EGID shall maintain such policies and procedures as necessary to restrict the accessibility, use and disclosure of PHI to non-covered components of OMES except as permitted by the Privacy Rule.

2.2. Protected Health Information and De-Identification

Release of individually identifiable PHI is restricted under HIPAA. Determinations by EGID as to whether health information is individually identifiable will be made based upon the standards contained in the Privacy Rule. Health information that meets the standards for de-identification is not subject to the Privacy Rule.

EGID shall adopt such procedures as necessary to ensure that re-identified PHI meets the standards of the Privacy Rule.

2.3. Maintaining Confidentiality of Health Information

EGID will not use or disclose PHI except as permitted or required by federal and state statutes or rules. Disclosure of PHI will be performed by trained personnel in accordance with applicable laws, regulations and EGID’s confidentiality policies.

2.3.1. Defining, Requesting and Maintaining Access to PHI

For all Confidential Information, EGID shall develop procedures to define the levels of access of users based upon their roles and responsibilities, process and review requests made for access, and ensure the users compliance with applicable policies to maintain access to the information.

2.3.2. Visitors and Vendors

EGID shall designate which workplace areas shall be considered non-secured, semi-secured, or secured. Non-secured areas are those areas in which no Confidential Information is accessible or discussed. Semi-secured areas may have some PHI in the vicinity but it is expected that non-employees will be in the area from time-to-time, and EGID employees must be alerted as to their presence.

Only current EGID employees, TPA representatives, or other persons approved by EGID senior management should be allowed in secured or semi-secured areas. Any other person, invited or otherwise authorized to enter EGID secured or semi-secured areas, but not formally associated with
EGID, must be accompanied and/or supervised by an EGID representative at all times. The representative is responsible for the actions of the visitor.

2.4. Verification of Identity and Authority

Prior to disclosing PHI, EGID personnel shall verify the identity and authority (where applicable) of the person or entity requesting the information.

2.5. Minimum Necessary Rule

EGID will make reasonable efforts to limit its disclosures and requests for PHI to the minimum necessary information needed to accomplish the purpose of the disclosure or request. For recurring processes, EGID will develop procedures and protocols that limit disclosures to the reasonably minimum amount required. All other requests will be reviewed on an individual basis to meet the minimum necessary requirement.

The minimum necessary rule is not required to be applied under the following circumstances:
1. For treatment;
2. To the individual;
3. In accordance with the individual’s valid authorization;
4. To the Office of Civil Rights for HIPAA compliance purposes; and
5. As required by law.

2.6. Awareness and Training

EGID shall train its workforce on its Confidentiality and Security of Information Policy. Training shall occur upon hiring and annually thereafter. Appropriate training shall also occur as necessary in a reasonably prompt timeframe for those workforce members whose job function has been affected as a result of material changes in the Confidentiality and Security of Information Policy or its associated procedures.

EGID’s Privacy Officer is charged with the overall responsibility of developing training programs and schedules to ensure that workforce members receive the training that is necessary and appropriate to perform their job functions in accordance with this policy.

On an ongoing basis, EGID will provide reminders about and awareness for confidentiality, privacy, and security of Confidential Information through a variety of modalities.

All employees will sign a confidentiality agreement upon hiring which states the importance, understanding, and the need for confidentiality. Employees agree not to disclose Confidential Information learned during the course of their employment with EGID, and further understand that Confidential Information disclosed during or after employment with EGID can result in legal actions.
Policy History

| Effective Date of Policy: March 1, 2013 | Date Policy Last Reviewed: January 28, 2013 |
| Next Scheduled Review: December 2013 | Date Policy Last Revised: January 28, 2013 |
| Approved by: OEIBB | Prior Policy: December 2, 2011 (OSEEGIB #102) |
| Approval Date: February 22, 2013 |  |
Section 3: Uses and Disclosures of PHI

3.1. General Rules

EGID will use and disclose PHI only as permitted or required under the Privacy Rule, and other federal or state laws and regulations.

3.2. Family Members and Friends

EGID may, but is not required to, disclose limited relevant PHI to a family member or friend who has been specifically identified by the member or who is directly involved in the care of the member, or the payment for care. Disclosure should only occur after verification of identity and authority, and should utilize the minimum necessary rule.

3.3. Authorizations

EGID may disclose PHI pursuant to an authorization provided by the member that satisfies all of the Privacy Rule’s requirements for a valid authorization. All uses and disclosures must be consistent with the terms and conditions of the authorization.

3.4. Legal, Specialized Government Functions, Workers’ Compensation, or Public Health Requests

PHI may be disclosed in the following situations without a Participant’s authorization, when certain requirements are satisfied. EGID shall have procedures describing the specific requirements that must be met before these types of disclosures may be made. The requirements shall include prior approval of EGID’s Privacy Officer or legal counsel. These disclosures are:

1. regarding victims of abuse, neglect or domestic violence;
2. for treatment purposes;
3. for judicial and administrative proceedings;
4. for law enforcement purposes;
5. for public health activities;
6. regarding an individual who has died;
7. for cadaveric organ-eye- or tissue-donation purposes;
8. for certain limited research purposes;
9. to avert a serious threat to health or safety;
10. for specialized government functions; and
11. that relate to workers’ compensation programs.

3.5. Limited Data Sets

EGID may release Limited Data Sets for purposes of research, public health or health care operations in accordance with procedures developed to implement 45 CFR 160.514(e)(3).
<table>
<thead>
<tr>
<th>Policy History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date of Policy: March 1, 2013</td>
</tr>
<tr>
<td>Next Scheduled Review: December 2013</td>
</tr>
<tr>
<td>Approved by: OEIBB</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Section 4: Participant’s Rights

4.1. The Notice of Privacy Practices

The Privacy Officer is responsible for developing and maintaining a notice of EGID’s privacy practices containing those provisions required by the Privacy Rule. The Notice of Privacy Practices outlines how EGID and its business associates will use and disclose individuals’ PHI and how individuals may gain access to that information.

EGID will maintain procedures and processes ensuring the availability and timely distribution of the notices, and that uses and disclosures of PHI are consistent with the contents of the notice.

4.2. Access to Personal Health Records

Except as provided by law, Participants have a right to access and obtain copies of their PHI that EGID (or its Business Associates) maintains in Designated Record Sets. EGID shall review such requests and approve or deny access based upon appropriate standards.

4.3. Restricting Use and Disclosure of PHI

Individuals may request restrictions on the use and disclosure of their PHI. Except as otherwise required under 45 CFR § 164.522, EGID does not have to grant these restrictions, but if it agrees to a restriction, it may not use or disclose the PHI in violation of the restriction, except in emergency situations. Any agreed-to restriction will not be effective to prevent uses and disclosures to the individual or as required by law. EGID may also prospectively terminate the agreed-to restriction.

4.4. Requesting a More Confidential Method of Communications

Participants have a right to request reasonable accommodations in receiving communications regarding their health information by alternative means or at an alternative location.

4.5. Amendment of Records

Individuals have a right under HIPAA to request that their PHI contained in a Designated Record Set be amended. EGID shall review such requests and based upon the factors involved either accept or deny the amendment.

4.6. Filing a Privacy Complaint

Participants have the right to file a formal complaint with EGID or with the Office of Civil Rights if the Participant believes that their privacy rights have been violated.
EGID shall provide a process for individuals to file complaints about the EGID’s policies, procedures, practices, and compliance with the Privacy Rule.

4.7. Accounting for Disclosures

A Participant has the right to obtain an accounting of certain disclosures of his or her own PHI within the last six years.

Policy History

<table>
<thead>
<tr>
<th>Effective Date of Policy: March 1, 2013</th>
<th>Date Policy Last Reviewed: January 28, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Scheduled Review: December 2013</td>
<td>Date Policy Last Revised: January 28, 2013</td>
</tr>
<tr>
<td>Approved by: OEIBB</td>
<td>Prior Policy: December 2, 2011 (OSEEGIB #102)</td>
</tr>
<tr>
<td></td>
<td>Approval Date: February 22, 2013</td>
</tr>
</tbody>
</table>
Section 5: Security of ePHI

5.1 Facility Access Controls

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate facility access security controls as required under 45 CFR §164.310(a).

5.2 Workstation Use and Security Access Controls

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate workstation use and security access controls to systems containing PHI as required under 45 CFR §164.310(b) and §164.310(c).

5.3 User Access Control

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate user access control to systems containing PHI to fulfill the requirements of 45 CFR §164.308(a) and §164.312(a).

5.4 Audit Controls

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate audit controls to systems containing PHI to fulfill the requirements of 45 CFR §164.312(b).

5.5 Device and Media Controls

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate device and media controls containing PHI to fulfill the requirements of 45 CFR §164.310(d).

5.6 Workforce Policies for Access to Systems with PHI

EGID shall have the responsibility to review OMES ISD appropriate workforce policies and procedures for those individuals who will access systems containing PHI to fulfill the requirements of 45 CFR §164.308(a).

5.7 Disaster Recovery / Contingency Planning

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate disaster recovery and contingency planning involving systems containing PHI as required under 45 CFR §164.308(a)(7).
5.8 Data Transmission Security

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network as required under 45 CFR § 164.312(e).

5.9 Risk Assessments: Security Management Process

EGID shall have the responsibility to review OMES ISD policies and procedures for the appropriate risk assessments of potential vulnerabilities to PHI and the purchase of systems and services necessary to protect PHI as required under 45 CFR § 164.308(a).

5.10 Periodic Security Evaluations

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate internal or external periodic evaluations of systems containing PHI as required under 45 CFR § 164.308(a)(8).

5.11 Security Incident Responses, Reporting and Mitigation

EGID shall have the responsibility to review OMES ISD policies and procedures for appropriate responses, reporting and mitigation of security incidents to systems containing PHI as required under 45 CFR § 164.308(a)(6).

5.12 Protecting ePHI From Improper Alteration or Destruction

EGID shall have the responsibility to review OMES ISD policies and procedures to protect ePHI from improper alteration or destruction as required under 45 CFR § 164.312(c).

5.13 Evaluating, Selecting, and Implementing Authentication Mechanisms

EGID shall have the responsibility to review OMES ISD policies and procedures for evaluating, selecting and implementing appropriate authentication mechanisms for ePHI as required under 45 CFR § 164.312(c).

Policy History

<table>
<thead>
<tr>
<th>Effective Date of Policy: March 1, 2013</th>
<th>Date Policy Last Reviewed: January 28, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Scheduled Review: December 2013</td>
<td>Date Policy Last Revised: January 28, 2013</td>
</tr>
<tr>
<td>Approved by: OEIBB</td>
<td>Prior Policy: December 2, 2011 (OSEEGIB #102)</td>
</tr>
<tr>
<td></td>
<td>Approval Date: February 22, 2013</td>
</tr>
</tbody>
</table>

12
Section 6: HIPAA Violations

6.1. Requirement to Report Violations to Privacy or Security Officer

All Business Associates, and all workforce members who have access to PHI, are required to report to the Privacy Officer any incidents involving possible breaches.

6.2. Risk Assessment of Breach

The Privacy Officer shall evaluate each reported violation of the Privacy Act in accordance with standards set forth by the Privacy Rule for the violation’s impact to the Participant and as to whether it is a breach that must be reported to the Secretary of the U. S. Department of Health and Human Services.

6.3. Required Individual Notifications for Privacy Breaches

For privacy breaches requiring notification, the Privacy Officer shall notify the affected individual without unreasonable delay, and in no case later than 60 days after discovery of a breach. An exception applies in the case of delays requested by law enforcement.

6.4. Notification to the Media

Except in situations of law enforcement delays, breaches of unsecured PHI involving more than 500 individuals shall be reported to prominent media outlets without unreasonable delay, and in no case later than 60 days after discovery of a breach.

6.5. Notification to the Secretary of HHS

EGID shall report all breaches of unsecured PHI to the Secretary of the U. S. Department of Health and Human Services as appropriate.

6.6. Notification by a Business Associate

EGID shall ensure that a process exists specifying regarding how, when and to whom a Business Associate should provide notification of a breach in order to expedite notification of affected Participants if necessary.

6.7. Law Enforcement Delay

EGID shall delay required notification of a breach at the request of a law enforcement official when such notification would impede a criminal investigation or cause damage to national security.
6.8. Burden of Proof

EGID shall maintain documentation of the evaluation of each reported breach and copies of the notifications that were made.

6.9. Disclosures by whistleblowers

In a whistleblower disclosure of PHI by a member of EGID’s workforce or of a Business Associate, EGID shall evaluate whether the particular disclosure is exempt from the Privacy Rule.

6.10. Disclosures by workforce members who are victims of a crime

A member of EGID’s workforce who is the victim of a criminal act may disclose limited PHI to a law enforcement official, provided that the PHI disclosed is about the suspected perpetrator of the criminal act.

6.11. Sanctions

EGID will apply appropriate sanctions against members of its workforce who fail to comply with the policies and procedures of this Confidentiality and Security of Information Policy.

6.12. Mitigation

EGID will mitigate, to the extent practicable, any harmful effect of a use or disclosure of protected health information in violation of its policies and procedures that is known to have been performed either by EGID or by EGID’s Business Associates. Factors which will be considered in the mitigation will include: whether any damage occurred; the nature and amount of damage, if it did occur; the nature of the PHI that was disclosed and the cause of disclosure; and the extent to which the harm can be mitigated.

6.13. Refraining from Intimidating or Retaliatory Acts

EGID will not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual who exercises any PHI privacy right under the Privacy Act, including the filing of a complaint with EGID or the Secretary of Health and Human Services and testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing associated with such complaint.
### Policy History

<table>
<thead>
<tr>
<th>Effective Date of Policy: March 1, 2013</th>
<th>Date Policy Last Reviewed: January 28, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Scheduled Review: December 2013</td>
<td>Date Policy Last Revised: January 28, 2013</td>
</tr>
<tr>
<td>Approved by: OEIBB</td>
<td>Prior Policy: December 2, 2011 (OSEEGIB #102)</td>
</tr>
<tr>
<td></td>
<td>Approval Date: February 22, 2013</td>
</tr>
</tbody>
</table>
Section 7: Business Associates

7.1. Safeguarding PHI

EGID shall ensure that Business Associates implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of EGID. The Business Associate shall ensure that proper security is in place to protect electronically stored health information.

7.2. Uses of PHI by the Business Associate

The Business Associate may only use and disclose the Participant’s PHI for the purposes of a Participant’s treatment, to facilitate payment for Plan benefits or for Business Associate business operations on behalf of the Participant. The Business Associate may not use or further disclose a member’s PHI other than permitted by EGID rules or policies, or as described in a written contract between EGID and the Business Associate, or as required by law.

The Business Associate shall establish procedures to protect a member’s health information and account for disclosures not authorized by these policies.

7.3. Access to PHI by Business Associate Employees

The Business Associate shall identify those of its employees who have a business need and authority to access a Participant’s PHI, and ensure that access is limited to those identified employees.

7.4. Safeguarding PHI by Agents or Subcontractors

Business Associates shall ensure that any agent or subcontractor to whom it provides PHI agrees to implement reasonable and appropriate safeguards to protect it.

7.5. Disclosure for Employment Related Actions

The Business Associate shall not use or disclose PHI for employment related actions concerning the Participant, unless required by law.

7.6. Notification of Breach

The Business Associate shall notify EGID within five [5] working days from when the Business Associate becomes aware of any use or disclosure of a Participant’s PHI that is inconsistent with this policy and make an accounting of these disclosures available for EGID and each affected Participant.

7.7. Access by Participants and Amendment of Records
The Business Associate shall allow a Participant to access and review health information on file with the Business Associate and submit amending statements for inclusion in their health information file.

7.8. Availability of Policies and Records to Authorities

The Business Associate shall make internal practices, books and records concerning uses and disclosures of protected health information available for inspection by the appropriate authority. A written contract between EGID and Business Associate shall not limit the Business Associate protection of a Participant’s PHI to an extent less than described in this policy.

7.9. Accounting for Disclosures of PHI

The Business Associate shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR§164.528.

7.10. Disposal of PHI

The Business Associate shall return to EGID or destroy a Participant’s PHI when no longer required by the Business Associate. If not feasible, the Business Associate shall limit the use or disclosure to the required purposes.

Policy History

<table>
<thead>
<tr>
<th>Effective Date of Policy: March 1, 2013</th>
<th>Date Policy Last Reviewed: January 25, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Scheduled Review: December 2013</td>
<td>Date Policy Last Revised: January 28, 2013</td>
</tr>
<tr>
<td>Approved by: OEIBB</td>
<td>Prior Policy: December 2, 2011 (OSEEGIB #102)</td>
</tr>
<tr>
<td></td>
<td>Approval Date: February 22, 2013</td>
</tr>
</tbody>
</table>
Section 8: Participating Entities

8.1. Status of Participating Entities

For purposes of HIPAA, EGID acts as a “fully insured plan” in relationship to its participating entities. EGID cannot disclose PHI for the purpose of employment related actions or decisions or in connection with any other benefit or employee benefit plan of the Participating Entity.

8.2. Status of OMES as an Employer

EGID cannot disclose PHI to any other division within OMES without the authorization of the Participant. EGID cannot disclose PHI for the purpose of employment related actions or decisions or in connection with any other benefit or employee benefit plan of OMES except those divisions operating as a Covered Entity.

Policy History

| Effective Date of Policy: March 1, 2013 | Date Policy Last Reviewed: January 28, 2013 |
| Next Scheduled Review: December 2013 | Date Policy Last Revised: January 28, 2013 |
| Approved by: OIEBB | Prior Policy: December 2, 2011 (OSEEGIB #102) |
| | Approval Date: February 22, 2013 |
Section 9: Other Privacy/Security Policies

9.1 Appointment of a Privacy Officer

In accordance with 45 CFR §164.530(a)(1), EGID shall designate a Privacy Officer who is responsible for the overall implementation and oversight of EGID’s Confidentiality and Security of Information Policy.

9.2 Appointment of a Security Officer

In accordance with 45 CFR §164.308(a)(2), EGID or OMES ISD shall designate a Security Officer who is responsible for the overall implementation and oversight of EGID’s efforts to prevent, detect, contain, and correct security violations.

9.3. Fund Raising

EGID shall not use or disclose PHI for purposes of fundraising.

9.4. Storing, Access, and Destruction of Confidential Records

All confidential records in all formats must be stored so that they are available for use, but also physically and technologically secure. Information and records must be protected from unauthorized access, physical damage or other reasonably foreseeable hazards.

EGID shall have procedures and processes in place to destroy confidential records in accordance with applicable standards.

Policy History

<table>
<thead>
<tr>
<th>Effective Date of Policy: March 1, 2013</th>
<th>Date Policy Last Reviewed: January 28, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Scheduled Review: December 2013</td>
<td>Date Policy Last Revised: January 28, 2013</td>
</tr>
<tr>
<td>Approved by: OEIBB</td>
<td>Prior Policy: December 2, 2011 (OSEEGIB #102)</td>
</tr>
<tr>
<td></td>
<td>Approval Date: February 22, 2013</td>
</tr>
</tbody>
</table>