EGYPTIAN ELECTRIC COOPERATIVE ASSOCIATION
POLICY BULLETIN NO. 214A

CASH AND BENEFITS PLAN (SECTION 125 PLAN)
HIPAA POLICIES AND PROCEDURES
EFFECTIVE DATE: APRIL 14, 2004

It is the intent of the Egyptian Electric Cooperative Association (EECA) to comply in all respects with the Privacy Rule. It is also the policy of EECA to comply with all relevant State laws governing health information privacy, to the extent those laws are not preempted by the Employee Retirement Income Security Act ("ERISA") or the Privacy Rule.

EECA has adopted this HIPAA Privacy Compliance Program, consisting of the attached Policies and Procedures, to ensure its compliance with the Privacy Rule and all applicable State laws governing health information privacy. Recognizing that conducting the Program is an evolving process, Egyptian Electric Cooperative Association will from time to time implement other Policies and Procedures and may modify existing Policies and Procedures to reflect its commitment to privacy and compliance with the Privacy Rule.

The HIPAA Privacy Compliance Program is not a statement of ideals: it is a detailed and specific statement of Policies and Procedures with which all personnel must comply. The HIPAA Privacy Compliance Program, and other information pertaining to Egyptian Electric Cooperative Association's protection of health information privacy, is at all times subject to inspection by the Secretary of HHS for the purpose of monitoring Egyptian Electric Cooperative Association's compliance with the Privacy Rule. All such requests for inspection should be directed to EECA's Privacy Officer.

The Privacy Rule is one of several proposed and final rules that are being published to implement the Administrative Simplification provisions of HIPAA. 45 C.F.R. Subchapter C, Parts 160 and 162, were added by the Final Rule at 65 Federal Register 50365 (Aug. 17, 2000). Part 160 comprises general provisions; Part 162 comprises various administrative simplification regulations relating to transactions and identifiers; Part 164 comprises the regulations implementing the security and privacy requirements of the legislation, the Privacy Rule [65 Federal Register 82462-82829 (December 28, 2000), as amended by 67 Federal Register 53182-53273 (August 14, 2002)].

A violation of the Privacy Rule could be extremely detrimental to EECA, its participants and beneficiaries, and its personnel. Failure to follow EECA's Privacy Policies and Procedures not only could lead to civil and criminal liability for you and EECA, but also could result in the termination of your employment. Therefore, it is imperative that all personnel comply with the standards contained in the HIPAA Privacy Compliance Program and related Policies and Procedures, immediately report any actual or potential violation of the Program to the Privacy Officer, and assist EECA in investigating any allegations of violations.

Potential Sanctions of Employees for Violations of the Privacy Rule

1. Penalties depend on the severity of the violation. Sanctions can range from a warning to immediate termination of employment and possible reporting to Federal and State administrative agencies.

2. Civil Sanctions. HHS may impose fines of $100 per violation, up to $25,000 per person per year, for negligent violation of a single standard.

3. Criminal Sanctions.

(a) HHS may make a criminal referral to the Department of Justice for any person who knowingly violates a standard, with potential fines of up to $50,000 and/or imprisonment for up to one year.

(b) Fines of up to $100,000 and/or imprisonment for up to five years may be imposed on any person who violates the standards under false pretenses.

(c) Fines of up to $250,000 and/or imprisonment for up to 10 years may be imposed on any person who violates any standard with the intent to sell, transfer or use health information protected under the Privacy Rule for commercial advantage.

****

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

POLICY:

EECA shall not use or disclose Protected Health Information (PHI) except as required or permitted by the Privacy Rule.

PROCEDURES:

(A) Uses and Disclosures for Health and Safety Purposes
All uses and disclosures of PHI for health and safety purposes must first be authorized by the Privacy Officer.

Such uses and disclosures include:

(1) Threat to Public Health or Safety
(2) Abuse, Neglect or Domestic Violence
(3) Public Health Activities
(4) Health Oversight Activities

(B) Uses and Disclosures Pursuant to Legal Proceedings and Law Enforcement
All uses and disclosures for legal and law enforcement purposes must first be authorized by the Privacy Officer.

(C) Uses and Disclosures Concerning Decedents
All uses and disclosures concerning decedents must first be authorized by the Privacy Officer.

(1) Post-mortem Identification, etc.
(2) Tissue Donation

(D) Uses and Disclosures for Other Government Purposes
All uses and disclosures for government purposes must first be authorized by the Privacy Officer. Once the use or disclosure is authorized, an Authorized Employee will use or disclose PHI under the following special circumstances:

(1) Armed Forces
(2) National Security
(3) Federal Protective Services
(4) Correctional Institution or Lawful Custody

(E) Uses and Disclosures for Workers' Compensation Purposes

All uses and disclosures for workers' compensation purposes must first be authorized by the Privacy Officer. Once the use or disclosure is authorized, an Authorized Employee will use or disclose PHI for compliance with workers' compensation and similar laws that provide benefits for work-related injuries or illnesses without regard to fault to the extent necessary for such compliance.

(F) Disclosures to Individuals

An Authorized Employee must disclose an individual's own PHI to the individual when requested by the individual, except information compiled in reasonable anticipation of or use in legal proceedings. Disclosures to individuals do not need to be recorded and will not need to be provided through an Accounting.

(G) Disclosures to Friends and Family Members

EECA will only disclose an individual's PHI to another person if EECA has a written Authorization from that individual permitting it to make such disclosure. Under limited circumstances EECA will disclose PHI to a family member, close personal friend or other person identified by the individual without an Authorization. Such disclosure is limited to PHI that is directly relevant to that person's involvement with the individual's care or payment for health care where at least one of the following conditions also is met:

(1) The individual agrees to the disclosure;
(2) The individual had an opportunity to agree or object* to the disclosure and did not object;
(3) Based on professional judgment and the circumstances, it can reasonably be inferred that the individual did not object to the disclosure; or
(4) If the individual was not available to agree or object, or cannot agree or object due to the individual's incapacity (i.e., due to an emergency situation), but the disclosure is in the individual's best interest.

*Opportunity to object, for these purposes, means the individual was present or otherwise available prior to the disclosure and had the capacity to make health care decisions. EECA also may use or disclose PHI to notify or assist in the notification of a family member, Personal Representative, another person responsible for the individual's care or a disaster relief organization of the individual's location, condition or death provided (1), (2), (3) or (4) above is satisfied. Uses and disclosures under these circumstances do not need to be recorded.

(H) Disclosures to Secretary of HHS

An Authorized Employee must disclose PHI to the Secretary of HHS when requested by the Secretary for purposes of determining EECA's compliance with the Privacy Rule.

(I) Disclosures to Another Health Plan

An Authorized Employee may disclose an individual's PHI to another Covered Entity as long as the disclosure is for Payment or certain Health Care Operation purposes, and only the minimum necessary is disclosed. If the disclosure is for reasons other than Payment or Health Care Operation purposes, an Authorization must first be obtained from the individual.

(J) Disclosures to Another Benefit Plan sponsored by EECA, other than the EECA default plan. An Authorized Employee may only disclose PHI to another benefit plan sponsored by EECA if an Authorization from the individual is received first. If possible, de-identified health information should be used instead of PHI. No authorization or de-identification of health information is necessary, however, if disclosure of PHI is made to the workers' compensation plan.

MINIMUM NECESSARY REQUIREMENTS

POLICY:

It is the Policy of EECA when using or disclosing Protected Health Information (PHI) or when requesting PHI from another Covered Entity, to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

PROCEDURES:

EECA shall use, disclose or request the minimum necessary amount of PHI in all situations, except the following:

(1) Disclosures made to the individual who is the subject of the PHI or pursuant to the individual's valid Authorization.
(2) Disclosures to the Secretary of Health and Human Services;
(3) Uses or disclosures that are required by law.
(4) Uses or disclosures that are required for EECA's compliance with applicable provisions of the Federal regulations governing health information systems.
(5) Uses or disclosures for which EECA has received an Authorization.

INDIVIDUAL AUTHORIZATION FOR CERTAIN USES AND DISCLOSURES

POLICY:

EECA will not use or disclose Protected Health Information (PHI) or request another Covered Entity to disclose PHI to EECA without the valid Authorization of the individual who is the subject of the PHI.

PROCEDURES:

(A) An Authorization must be in writing and complete, not be expired or known by EECA to have been revoked, not contain any material information known by EECA to be false, not impermissibly condition enrollment or eligibility for benefits on the Authorization, and not be combined with any other document.

(B) Each signed Authorization must be given to the Privacy Officer who will retain the Authorization for a period of at least six years from the later of the effective date or the expiration date.

(C) The Privacy Officer will provide the individual with a copy of the Authorization.

(D) An individual may revoke an Authorization in writing at any time except to the extent that EECA already has acted in reliance on the Authorization or, if the Authorization was a condition for enrollment under an insurance contract, where the insurer has the legal right to

contest a claim. The individual must deliver the written Revocation Notice to the Privacy Officer who will notify the relevant Authorized Employee(s) and retain the revocation for a period of at least six years from its effective date.

PERSONAL REPRESENTATIVES OF INDIVIDUALS

POLICY:

It is the Policy of EECA to treat an individual's Personal Representative as the individual with respect to the Protected Health Information (PHI) of the individual, except as otherwise provided in this policy. The Personal Representative of an individual is a person who, under applicable State law, has the authority to act on behalf of the individual in making decisions related to health care.

PROCEDURES:

Prior to allowing a person to act as an individual's Personal Representative in connection with EECA's use or disclosure of the individual's PHI, EECA must determine if the individual is

(a) an adult or emancipated minor;
(b) an unemancipated minor;
(c) deceased;
(d) a victim of abuse, neglect or endangerment.

EECA must obtain written documentation of a person's authority under applicable State law to act as the individual's Personal Representative before allowing the person to act as the individual's Personal Representative in connection with the use or disclosure of the individual's PHI.

A Personal Representative Form must be completed and sent to EECA's Privacy Officer. The Privacy Officer will approve or deny the Personal Representative of an Individual Form. Upon approval, EECA shall maintain in the individual's claim record the written documentation of a person's authority to act as the individual's Personal Representative. EECA shall also maintain in the individual's claim record the Personal Representative's name, address, telephone number and relationship to the individual.

DISCLOSURES OF DE-IDENTIFIED PROTECTED HEALTH INFORMATION

POLICY:

EECA may disclose de-identified Protected Health Information (PHI). De-identified PHI is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

EECA may use PHI to create de-identified health information or to disclose PHI to a Business Associate to use to create de-identified health information.

EGYPTIAN ELECTRIC COOPERATIVE ASSOCIATION
POLICY BULLETIN NO. 214A

SAFEGUARDING PROTECTED HEALTH INFORMATION

POLICY:

The Privacy Officer and other Authorized and Responsible Employees must take reasonable steps to ensure that Protected Health Information (PHI) is not intentionally or unintentionally used or disclosed in any manner not consistent with these Privacy Policies and Procedures. Such steps include securing PHI using administrative, physical and electronic access barriers; destroying documents containing PHI that do not need to be retained; training Authorized Employees regarding privacy policies; and limiting the number of persons included as Authorized Employees. Physical access to areas containing PHI will be limited, wherever possible, to Authorized Employees only.

PROCEDURES:

(A) Printed Materials

Authorized Employees must store all printed materials containing PHI in secure locations when not in use. When printed materials are in use, the Authorized Employee must take reasonable steps to ensure that these materials are viewable only by the Authorized Employee. At no time should the files remain unlocked when the Authorized Employee has left the office premises. Under no circumstances should any files containing PHI be taken off the office premises. EECA's Privacy Officer must be notified prior to providing PHI for a legal or administrative proceeding. Within the Human Resources Department, PHI should be filed in a separate benefits file and only Authorized HR employees should have access to these files. Under no circumstances should PHI be maintained in an employee's personnel file. Mail addressed to Authorized Employees who regularly receive mail containing PHI should be unsealed only by that addressee. Mail should be left in a mail slot belonging only to that Authorized Employee. If an Authorized Employee knows that an individual will be sending PHI through the mail, the Authorized Employee will instruct that individual send the information to his/her attention and to mark the envelope "personal." If an Authorized Employee is sending PHI to an individual, he/she shall mark the envelope "personal" and shall verify the individual's address prior to mailing it.

If printed material no longer needs to be retained after use, it should be properly destroyed (i.e., shredded) by the Authorized Employee, unless subject to Record Retention.

(B) Facsimile Machines and Printers/Copiers

Authorized Employees must take reasonable steps to ensure that all incoming facsimiles and print jobs containing PHI are viewable and retrievable only by the Authorized Employee with a legitimate need to know. If a fax or copy no longer needs to be retained after use, it should be destroyed, unless subject to Record Retention.

(C) Telephonic and Other Verbal Communication

Authorized Employees must take reasonable steps to ensure that telephone and other verbal conversations in which PHI is discussed are not overheard by persons, who do not have a legitimate need to know the content of the conversation. A voice-mail message containing PHI is not permitted and should not be left on an answering machine. When receiving a voice message, an Authorized Employee should not use a speakerphone unless there are other Authorized Employees who need to hear the message in order to perform their job or a necessary function. When speaking with an individual on the phone about PHI, the Authorized Employee will take reasonable steps to ensure that the individual is actually who they say they are. If an Authorized Employee is unable to verify the identity of the individual, no PHI will be discussed on the telephone.

(d) Office Safeguards

(1) IT Security
Only Authorized Employees with appropriate clearance will be provided access to PHI. Any outside entity performing operating and maintenance services on computer hardware or software containing PHI will be monitored.

(2) After Hours
(a) The Human Resources Department will be secured and locked during non business hours.
.
(b) All Authorized Employees are required to clear their desks of PHI and secure all PHI information before leaving the office premises.

(3) Termination
When a Responsible Employee or an Authorized Employee who has access to PHI is terminated, their access to PHI shall immediately be terminated. If the terminated employee has a key or access card, it will be immediately retrieved from the terminated employee.

(4) Guests/Temporaries/Consultants
No guest shall be permitted to enter areas where PHI is located unless escorted by an Authorized Employee. Temporaries and consultants are to be closely supervised and placed in a work area where they do not have access to PHI.

ADMINISTRATIVE REQUIREMENTS

POLICY:

EECA shall comply with the Administrative Requirements under the Privacy Rules.

PROCEDURES:

(A) Privacy Officer and Contact Person Appointment
The Privacy Officer will either perform the following, or designate an Authorized Employee to perform the following:
(1) Develop, implement and update Plan Privacy Policies and Procedures;
(2) Ensure appropriate privacy training for Authorized Employees;
(3) Investigate and respond to individuals' complaints regarding impermissible uses or disclosures of PHI and related policy violations;
(4) Provide individuals with a Privacy Notice and information regarding Plan Policies and Procedures related to PHI; and
(5) Maintain documentation of policies, notices, complaints and related activities consistent with record retention.

(B) Designating Authorized and Responsible Employees
The Privacy Officer will be responsible for identifying those employees that will be designated as Authorized Employees, and will be responsible for informing such employees which uses and disclosures of PHI are permissible with respect to that Authorized Employee's duties and responsibilities related to EECA. The Privacy Officer will also designate which employees will be Responsible Employees, and will inform such employees which uses and disclosures are permissible and impermissible. No employees other than Authorized or Responsible Employees

should have access, accept receipt, record or transmit PHI, other than PHI that relates directly to that employee as an individual.

(C) Employee Training

The Privacy Officer will ensure that all existing Authorized Employees are trained in and new Authorized Employees must be trained within a reasonable time after beginning to work as an Authorized Employee. The level of training will depend upon the Authorized Employee's access to PHI. The Privacy Officer must maintain a record of all such training consistent with the Record Retention procedures.

(D) Remedies for Violations of Protected Health Information Privacy Policies and Procedures

(1) Complaints

Any complaints regarding these Policies and Procedures or other report of impermissible uses or disclosures of PHI shall be forwarded to the Privacy Officer. Such complaints will be promptly investigated. Any Authorized or Responsible Employee who violates a Privacy Policy or Procedure will be subject to disciplinary action up to and including discharge.

(2) Mitigation

An Authorized Employee is required to mitigate harm resulting from an impermissible use or disclosure of PHI. If an Authorized Employee is aware of an impermissible use or disclosure, he/she will report in writing the impermissible use or disclosure to the Privacy Officer immediately and shall cease the use or practice that resulted in an impermissible use or disclosure. If the Authorized Employee fails to report the impermissible use or disclosure and/or ceases to take any action to mitigate the harm of such an impermissible use or disclosure, the employee will be subject to disciplinary action.

(3) Intimidation or Retaliation

An Authorized or Responsible Employee who intimidates or retaliates against an individual for exercising his or her HIPAA rights shall be subject to disciplinary action.

(4) Penalties for Non-Compliance

If an employee violates HIPAA's privacy protections, HHS will impose civil penalties from $100 per incident up to $25,000 per person, per year, per violation. Knowing violations of HIPAA can result in the employee going to jail for up to ten (10) years and fines up to $250,000. In addition, criminal penalties may be imposed by HHS up to $50,000 and up to one (1) year imprisonment for obtaining or disclosing PHI; up to $100,000 and up to five (5) years in prison for obtaining PHI under false pretenses; and up to $250,000 and up to ten (10) years imprisonment for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

(5) Reporting Policy Violations

Each Authorized or Responsible Employee must promptly report violations of these Policies and Procedures to the Privacy Officer.

(6) Written Policies and Procedures

These comprehensive Privacy Policies and Procedures shall be maintained at all times by EECA. The Privacy Officer shall be responsible for amending these Policies and Procedures. The Privacy Officer shall ensure that all amendments are in writing and communicated to Authorized Employees, Responsible Employees and other necessary parties. The Privacy Officer shall enforce and ensure that all Authorized and Responsible Employees adhere to these written Policies and Procedures. If an unforeseen circumstance requires a change from

these written Policies and Procedures, the Privacy Officer shall decide whether or not to grant an exception from complying with the requirements herein. Although these Policies and Procedures are designed to comply with HIPAA, if there is a more restrictive State law, that law will be followed instead of HIPAA.

RECORD RETENTION

POLICY:

The Privacy Officer must retain the following records either in paper or electronic form for six years from the date of creation or the date when it was last in effect, whichever is later: Privacy Policies and Procedures, Authorizations and Revocations, training records, designation of Privacy Officer, complaints and related investigations and sanctions, requests for restrictions on uses and disclosures, and uses and disclosures of Protected Health Information (PHI) subject to an Accounting.

TRAINING OF EMPLOYEES

POLICY:

It is the Policy of EECA to train all of its Authorized Employees concerning the Policies and Procedures regarding Protected Health Information (PHI), as necessary and appropriate for these employees to carry out their specific functions with respect to Plan Payment or Health Care Operations. The term "Authorized Employees," as used in this policy, means all individuals who are under the control of EECA and are described in the Plan documents as persons authorized to have access to or receive PHI on behalf of EECA.

PROCEDURES:

(A) Current Authorized Employees
EECA will provide training to all current Authorized Employees involved in Plan Administration functions no later than April 14, 2004. All such employees will be expected to attend such training programs. Attendance will be recorded to ensure that all Authorized Employees have received sufficient training. EECA will provide updated training to Authorized Employees on a yearly basis, or in accordance to any material revisions to the Privacy Rule regulation.

(B) New Authorized Employees
As part of orientation for each new employee, the Human Resources Department will include in the new employee's benefit package the HIPAA Summary and Privacy Notice. In addition, the Privacy Officer will train new Authorized Employees involved in Plan administration functions of EECA's Policies and Procedures regarding the handling of PHI. Such training will occur within 45 days after the Authorized Employee joins EECA's workforce.

(C) Changes in Policies and Procedures Regarding Protected Health Information EECA will train each Authorized Employee whose functions are affected by a material change in EECA's Policies or Procedures regarding PHI within a reasonable period of time, but in no event longer than 60 days after the final rule change becomes effective. EECA will conduct programs covering such changes on a regular basis.

(D) Documentation and Certification

EECA will document the time, date, place and content of each training session, as well as the attendees at each training session. Such documentation will be maintained by the Privacy Officer in EECA's HIPAA compliance files. In addition, EECA will require all Authorized Employees to execute a Certification of Training. EECA will maintain all Certifications in its HIPAA compliance files and in each employee's respective personnel file maintained by EECA and will make them available for inspection to regulatory authorities, as appropriate.

CONTRACTS WITH BUSINESS ASSOCIATES

POLICY:

It is the Policy of EECA to disclose Protected Health Information (PHI) to a Business Associate or to allow a Business Associate to create or receive Protected Health Information on behalf of EECA only if there is a written contract in effect between the Business Associate and EECA ("Business Associate Contract") which includes provisions in substantially the form set forth in this Policy.

REVIEW AND RESOLUTION OF COMPLAINTS

POLICY:

It is the Policy of EECA to provide a process for individuals to make complaints concerning the compliance with the Federal Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. §164.500 *et seq*. ("Privacy Rule"), EECA's Policies and Procedures adopted in connection with the Privacy Rule ("HIPAA Policies") and compliance with its HIPAA Policies and Procedures. It is also the Policy of EECA to review and resolve any complaints it receives regarding the Plan's compliance with the Privacy Rule and its HIPAA Policies and Procedures (collectively, "Privacy Complaints").

PROCEDURES:

(A) Contact Information

All Privacy Complaints that EECA receives shall be forwarded to the Privacy Officer as follows:

Egyptian Electric Cooperative Association
Attention: Privacy Officer
1005 W. Broadway, P. O. Box 38
Steeleville, IL 62288

Telephone: (618) 965-3434
Fax: (888)712-8383
Email: dluehr@eeca.coop

(B) Privacy Complaint Log

The Privacy Officer shall document the following with respect to each Privacy Complaint received:

(1) The date the Privacy Complaint was received;
(2) If the Privacy Complaint is received orally, a description of the complaint will be documented. The Privacy Officer will request a written complaint from the individual;
(3) A copy of the requested written Privacy Complaint will be filed;
(4) A copy of the written statement will also be provided to the individual making the Privacy

Complaint

(C) Responsible Party to Investigate and Resolve Complaint
EECA has established a Privacy Complaint Committee to review and resolve any Privacy Complaints that the Privacy Officer receives.

(D) Time Frame for Resolution
(1) Investigation
Within 30 days after the Privacy Officer receives a Privacy Complaint, the Privacy Complaint Committee must investigate the underlying circumstances relating to the Privacy Compliant.
(2) Resolution
Within 60 days after the Privacy Officer receives a Privacy Complaint, the Privacy Complaint Committee must provide a written response to the individual who submitted the Privacy Complaint containing the following information:

(a) The name of an EECA contact person who will answer questions relating to the investigation and resolution of the Privacy Complaint;
(b) A general description of the steps taken to investigate the Privacy Complaint;
(c) An explanation of EECA's resolution regarding the Privacy Complaint; and
(d) The date of completion of the investigation of the Privacy Complaint.

(E) Document Retention
EECA shall retain copies of the documentation listed in Section B for a period of six years from the date that the Privacy Complaint Committee provides the individual the written response described in section D (2) above.

Adopted: April 27, 2004
Revised: 03/27/2012
Revised: 09/30/2014

Attested: Allen Haake, Secretary
Attested: Kevin Liefer, Secretary