HANCOCK HOLDING COMPANY AND SUBSIDIARIES
ORGANIZED HEALTH CARE ARRANGEMENT
HIPAA SECURITY POLICIES AND PROCEDURES

(Amended and Restated Effective September 23, 2013)

1. General:

Hancock Holding Company and its subsidiaries (collectively, the **"Plan Sponsor"**) adopted HIPAA Security Policies and Procedures (the **"Security Policies and Procedures"**), which were first effective on April 20, 2005, in accordance with Title II of the Health Insurance Portability and Accountability Act of 1996 (**"HIPAA"**) and the regulations promulgated thereunder (collectively the **"Security Rule"**). These Security Policies and Procedures are hereby amended and restated in their entirety to comply with the requirements of HIPAA, the Health Information Technology for Economic and Clinical Health Act (the **"HITECH Act"**), and their implementing regulations and guidance and are intended to be construed and interpreted in accordance with such laws respect to the confidentiality, integrity and availability of Electronic Protected Health Information ("EPHI").

The Plan Sponsor has designated the health plans maintained by the Plan Sponsor and its subsidiaries as an Organized Health Care Arrangement ("OHCA") as outlined and updated in Exhibit A hereto. References to the OHCA in these Security Policies and Procedures shall include all health plans identified as members of such arrangement. Such designation describes any joint compliance activities to be undertaken by the members of the OHCA. The members of the OHCA are covered entities, as defined by HIPAA, and are subject to the HIPAA Security Rule. These HIPAA Security Policies and Procedures are intended to coordinate with the HIPAA Privacy Policies and Procedures adopted by the OHCA. Key terms, which supplement those previously defined in the HIPAA Privacy Policies and Procedures, are defined in Section 7 of these HIPAA Security Policies and Procedures.

These HIPAA Security Policies and Procedures are also intended to coordinate with the Hancock Holding Company, Inc. Comprehensive Information Security Program ("Hancock Information Security Policies") previously adopted by the Plan Sponsor. The references throughout these HIPAA Security Policies and Procedures to existing policies and procedures are referring to the Hancock Information Security Policies which are adopted by the OHCA with regard to EPHI which is collected, maintained, stored, used, or transmitted by the Plans that are members of the OHCA. Any amendments to the Hancock Information Security Policies will apply for purposes of these HIPAA Security Policies and Procedures to the extent they impact information which includes EPHI and are not otherwise specifically addressed by these HIPAA Security Policies and Procedures.

The Plan Sponsor reserves the right to modify or amend these HIPAA Security Policies and Procedures, including the Exhibits hereto, subject to and consistent with any limitations imposed by applicable law. The Plan Sponsor may also supplement these HIPAA Security Policies and Procedures with more specific Exhibits addressing the operations of administering the HIPAA Security Rule as the various HIPAA Security Policies and Procedures are implemented.

2. Security Standards and Implementation Specifications Under the HIPAA Security Rule

The Plan Sponsor shall implement all administrative, physical, and technical safeguards of EPHI as required by the HIPAA Security Rule. The Plan Sponsor shall implement all required implementation specifications. The Plan Sponsor shall implement addressable implementation specifications as follows:

a. If a given addressable implementation specification is determined to be reasonable and appropriate, the Plan Sponsor shall implement it.

b. If a given addressable implementation specification is determined to be an inappropriate and/or unreasonable security measure for the Plan Sponsor, but the standard cannot be met without implementation of an additional security safeguard, the Plan Sponsor shall implement an alternate measure that accomplishes the same end as the addressable implementation specification.

c. If a given addressable implementation specification is determined to be inapplicable (that is, neither reasonable nor appropriate) and the standard can be met without implementation of an alternative measure, the Plan Sponsor shall document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met.

3. Administrative Safeguards of EPHI:

a. *Security Management* – The Plan Sponsor has previously adopted and implemented a policy for Information Systems Security Incidents and procedures to prevent, detect, contain, and correct security violations as part of the Hancock Information Security Policies.

i. Risk Analysis – The Plan Sponsor shall assess at least annually the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by the OHCA.

ii. Risk Management – The Plan Sponsor has implemented security measures sufficient to reduce risks and vulnerabilities for EPHI to a reasonable and appropriate level.

iii. Sanction Policy – The HIPAA Security Official (as designated in Exhibit B hereto) is authorized to sanction any employee of the Plan Sponsor that violates these HIPAA Security Policies and Procedures. Any violation of these HIPAA Security Policies and Procedures should be reported directly to the HIPAA Security Official. The HIPAA Security Official shall investigate any alleged violation. Sanctions shall be imposed by the HIPAA Security Official and shall be consistent with the Plan Sponsor's existing disciplinary policy.

iv. Information System Activity Review – The Plan Sponsor has implemented procedures with regard to EPHI to regularly review records of information system activity, including audit logs, access reports, and Security Incident tracking reports.

b. *Assigned HIPAA Security Responsibility* – The Plan Sponsor has identified, on Exhibit B hereto, the HIPAA Security Official responsible for the continued development and implementation of these HIPAA Security Policies and Procedures. The HIPAA Security Official's job description is set forth in Exhibit C hereto. The HIPAA Security Official may delegate one or more of the duties hereunder to any other employee or officer of the Plan Sponsor. In carrying out his or her duties hereunder, the HIPAA Security Official shall be entitled to engage such attorneys (who may include attorneys for the Plan Sponsor, whether employees or otherwise), consultants, or other experts as it deems necessary or advisable.

c. *Workforce Security* – The Plan Sponsor has identified "Necessary Employees" (in Exhibit B hereto) who shall be those employees and officers of the Plan Sponsor who have access to EPHI as required to establish, maintain, and administer the Plan and the other plans in the OHCA. Necessary Employees may be designated individually or by title or group. The Plan Sponsor shall designate the types of EPHI to which Necessary Employees need access to carry out their duties relating to the OHCA. EPHI shall be accessed only by Necessary Employees.

   i. Authorization and/or Supervision – The Plan Sponsor has implemented procedures for the authorization and/or supervision of workforce members who work with EPHI and the locations where it may be accessed.

   ii. Workforce Clearance Procedure – The Plan Sponsor has implemented procedures to determine that the access of a workforce member to EPHI is appropriate.

   iii. Termination Procedures – The Plan Sponsor has implemented procedures for terminating access to EPHI when the employment of a workforce member ends or when such employee is no longer entitled to access EPHI.

d. *Information Access Management* – The Plan Sponsor has implemented policies and procedures for authorizing access to EPHI that are consistent with the HIPAA Security Rule.

   i. Access Authorization – The Plan Sponsor has implemented policies and procedures for granting access to EPHI through access to a workstation, transaction, program, process, or other mechanism.

   ii. Access Establishment and Modification – The Plan Sponsor has implemented policies and procedures that establish, document, review and modify a user's right of access to a workstation, program, or process.

e. *Security Awareness and Training* – The Plan Sponsor has implemented a HIPAA security awareness and training program, as set forth in Exhibit D hereto, for members of its workforce, including management. All Necessary Employees will be informed and/or trained periodically in the following areas: (1) all of the OHCA's Security Policies and Procedures, or if appropriate, relevant policies and procedures for any particular employee if his or her job responsibilities do not necessitate training in all of the Security Policies and Procedures; (2) the

administrative, physical, and technical safeguards implemented by the Plan Sponsor to secure the confidentiality, integrity, and availability of Electronic Protected Health Information; (3) relevant provisions of the Security Rule; and (4) the requirement that all employees report any Security Incidents, whether caused by workforce member or a Business Associate, to the Security Official. The Security Official will maintain records indicating who has been trained, what training occurred, and the date of training, for six years following the date of the training.

i. Security Reminders – The Plan Sponsor has implemented periodic security updates.

ii. Protection from Malicious Software – The Plan Sponsor has implemented procedures for guarding against, detecting, and reporting Malicious Software.

iii. Log-In Monitoring – The Plan Sponsor shall track each Necessary Employee's access to EPHI. The Plan Sponsor has implemented procedures for monitoring log-in attempts and reporting discrepancies.

iv. Password Management – Necessary Employees have been assigned a password. The Plan Sponsor has implemented procedures for creating, changing, and safeguarding passwords.

f. *Security Incident Procedures* – The Plan Sponsor has implemented policies and procedures to address Security Incidents.

i. Investigation – The HIPAA Security Official shall identify and respond to suspected or known Security Incidents, as detailed in Exhibits E and F hereto.

ii. Mitigation – The HIPAA Security Official shall mitigate, to the extent reasonably practicable, any harm caused by a violation of these HIPAA Security Policies and Procedures. Upon learning of a violation of these HIPAA Security Policies and Procedures, the HIPAA Security Official shall determine whether a participant or beneficiary could be or has been harmed by the violation and whether there are any practicable steps that might have a mitigating effect with regard to such harm.

iii. Documentation – The HIPAA Security Official shall document Security Incidents and their outcomes. Such documentation may include amending these HIPAA Security Policies and Procedures; sanctioning employees and/or Business Associates involved in the Security Incident; and conducting further training which is intended to ensure that the Security Incident does not recur.

g. *Contingency Plan* – The Plan Sponsor shall review existing policies and establish and implement, as needed, additional policies and procedures for responding to an emergency or other occurrence, such as fire, vandalism, system failure and natural disaster, that damages systems that contain EPHI.

i. Data Backup Plan – The Plan has established and implemented procedures to create and maintain retrievable exact copies of EPHI.

ii. Disaster Recovery Plan – The Plan Sponsor shall review existing procedures and establish and implement, as needed, additional procedures to restore any loss of data.

iii. Emergency Mode Operation Plan – The Plan Sponsor shall review existing procedures and establish and implement, as needed, additional procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

iv. Testing and Revision Procedures – The Plan Sponsor has implemented procedures for periodic testing and revision of contingency plans.

v. Applications and Data Criticality Analysis – The Plan Sponsor shall assess the relative criticality of specific applications and data in support of other contingency plan components.

h. *Evaluation of Security Policies* – The Plan Sponsor shall perform periodic technical and non-technical evaluations, based initially upon the standards implemented under the HIPAA Security Rule and subsequently in response to environmental or operational changes affecting the security of EPHI, that establish the extent to which the Plan Sponsor's HIPAA Security Policies and Procedures meet the requirements of the HIPAA Security Rule.

i. *Business Associate Contracts and Other Arrangements* – The Plan Sponsor has entered into (or is in the process of entering into or amending) written Business Associate Agreements with the Business Associates identified in Exhibit B hereto. The Agreements permit the Plan Sponsor's Business Associates to create, receive, maintain, or transmit EPHI on the Plan Sponsor's behalf. Each Business Associate Agreement provides that the Business Associate shall:

i. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains or transmits on behalf of the Plan Sponsor;

ii. Ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it;

iii. Report to the Plan Sponsor any Security Incident of which it becomes aware; and

iv. Authorize termination of the Agreement by the Plan Sponsor if the Plan Sponsor determines that the Business Associate has violated a material term of the Agreement.

4. Physical Safeguards of EPHI:

a. *Facility Access Controls* – The Plan Sponsor has implemented policies and procedures to limit physical access to its electronic information systems

containing EPHI and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

i. Contingency Operations – The Plan Sponsor has established and is implementing procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

ii. Facility Security Plan – The Plan Sponsor has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

iii. Access Control and Validation – The Plan Sponsor has implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.

iv. Maintenance Records – The Plan Sponsor has implemented policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (i.e., hardware, walls, doors and locks).

b. *Workstation Use* – The Plan Sponsor has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.

c. *Workstation Security* – The Plan Sponsor has implemented physical safeguards for all workstations that access EPHI necessary to restrict access to authorized users.

d. *Device and Media Controls* – The Plan Sponsor has implemented policies and procedures that govern the receipt and removal of hardware and Electronic Media that contain EPHI into and out of a facility and the movement of these items within the facility.

i. Disposal – The Plan Sponsor has implemented policies and procedures necessary to address the final disposition of EPHI and/or the hardware or Electronic Media on which it is stored.

ii. Media Re-Use – The Plan Sponsor has implemented procedures necessary for removal of EPHI from Electronic Media before the media is made available for reuse.

iii Accountability – The Plan Sponsor shall maintain records regarding the movements of hardware and Electronic Media and any person responsible therefore.

iv. Data Backup and Storage – The Plan Sponsor shall create a retrievable, exact copy of EPHI, when needed, before movement of equipment.

5. Technical Safeguards of EPHI:

a. *Access Control* – The Plan Sponsor has implemented technical policies and procedures for electronic information systems that maintain EPHI necessary to allow access only to those persons or software programs that have been granted access rights.

i. Unique User Identification – The Plan Sponsor has assigned a unique User-id and password to each Necessary Employee authorized to access EPHI. Such User-id password shall be used to track each such Necessary Employee's access to EPHI.

ii. Emergency Access Procedure – The Plan Sponsor shall review, establish, and implement, as needed, procedures for obtaining necessary EPHI during an emergency.

iii. Automatic Logoff – The Plan Sponsor has implemented procedures that terminate an electronic session after a predetermined time of inactivity.

iv. Encryption and Decryption – The Plan Sponsor has implemented a mechanism to encrypt and decrypt EPHI.

b. *Audit Controls* – The Plan Sponsor has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

c. *Integrity* – The Plan Sponsor has implemented policies and procedures to protect EPHI from improper alteration or destruction.

i. Mechanism to Authenticate EPHI – The Plan Sponsor has implemented electronic mechanisms necessary to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

d. *Person or Entity Authentication* – The Plan Sponsor has implemented procedures necessary to verify that a person or entity seeking access to EPHI is the one claimed.

e. *Transmission Security* – The Plan Sponsor has implemented technical security measures necessary to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

i. Integrity Controls – The Plan Sponsor has implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until its disposal.

ii. Encryption – The Plan Sponsor has implemented a mechanism to encrypt EPHI whenever deemed appropriate.

6. Record Retention

The HIPAA Security Official shall retain all records required to be retained under the HIPAA Security Rule for a period of six years, including, without limitation:

a. Documents regarding the Plan Sponsor's assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI;

b. Documents regarding the Plan Sponsor's decision to forego the adoption of an addressable implementation specification in favor of an alternate security measure or no measure;

c. Documents regarding the amendment or modification of these HIPAA Security Policies and Procedures;

d. Audit logs, access reports, and Security Incident tracking reports;

e. Documents regarding the HIPAA training of employees;

f. Documents regarding repairs and modifications to the physical components of a facility which are related to security; and

g. Documents regarding the movement of hardware and Electronic Media and any person responsible therefore.

The six year period shall be measured from the date of the document's creation or the date when it was last in effect.

7. Definitions

The key terms under these HIPAA Security Policies and Procedures are aligned with key terms under HIPAA Privacy Policies and Procedures (like covered entity, business associate, protected health information). Additional key terms used in these HIPAA Security Policies and Procedures are as follows:

a. *Electronic Media* means:

i. Electronic Storage Media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card; or

ii. Transmission Media used to exchange information already in electronic storage media, including the internet, extranet, leased lines, dial-up lines, private networks and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmission via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

b. *Electronic Protected Health Information* ("EPHI") means protected health information ("PHI") that is or has been transmitted via Electronic Media or maintained in Electronic Media.

c. *Malicious Software* means software (like a virus) designed to damage or disrupt a system.

d. *Security Incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

HANCOCK HOLDING COMPANY AND SUBSIDIARIES
HIPAA SECURITY POLICIES AND PROCEDURES

EXHIBIT A
Organized Health Care Arrangement

1. **Designation of the Health Plans constituting the organized health care arrangement:**

Plan Name	**Plan No.**	**Plan Sponsor**
Employee Health Protection Plan for Hancock Holding Company (includes self-insured portion)	507	Hancock Holding Company
Hancock Holding Company Cafeteria Plan (Health Care Spending Account)	779	Hancock Holding Company
Employee Assistance Program ("EAP")	N/A	Hancock Holding Company

2. **Designate the joint HIPAA compliance functions:**

Function	**Health Protection Plan**	**EAP**	**Cafeteria Plan Health Care Spending Account**
Policies and Procedures	Yes	Yes	Yes
Security Official	Yes	Yes	Yes
Training	Yes	Yes	Yes
Plan Amendment	Yes	Yes	Yes
Administrative Safeguards	Yes	Yes	Yes
Physical Safeguards	Yes	Yes	Yes
Technical Safeguards	Yes	Yes	Yes
Records Retention	Yes	Yes	Yes
Business Associate Agreements	Yes	Yes	Yes

HANCOCK HOLDING COMPANY AND SUBSIDIARIES
HIPAA SECURITY POLICIES AND PROCEDURES

EXHIBIT B
Designation of HIPAA Security Official, Necessary Employees, And Business Associates

1. **HIPAA Security Official:** The HIPAA Security Official shall be the Manager—Information Security.

2. **Necessary Employees:** The Necessary Employees and their restrictions and limitations with respect to EPHI shall be:

Name/Title	**Functions/Limitations**
Manager – Benefits	Plan Administration, Plan Design, Appeals
Benefits Administrator	Plan Administration
HR Service Center Manager	Plan Administration
HR Service Center Representative	Plan Administration
HR Service Center Specialist	Plan Administration
Director of HR Shared Services	Plan Design, Plan Administration, Appeals
HR Associate	Files HR documents which include Plan information
Payroll	Premium deductions, plan enrollment information
HRIS Analyst	Administration of safeguards
Associate Relations	Premium deductions, plan enrollment information
Recruiting	Premium deductions, plan enrollment information

The titles set forth above are current as of June 15, 2014. The Plan Sponsor will review and update the designation of Necessary Employees annually. However, any change in the above titles that does not impact a Necessary Employee's need to access PHI and/or e-PHI to perform his or her job duties will be deemed to be incorporated based on his or her original designation as a Necessary Employee.

In addition to the job titles listed above, members of the IT Department who have been identified as Necessary Employees are listed on the attached Addendum to these Security Policies and

Procedures. Regardless of designation as a Necessary Employee, all associates in the IT Department will be required to complete HIPAA Security training to ensure that they are aware of the Company's policies regarding safeguards for e-PHI.

3. **Business Associates:** The Business Associates of the OHCA are listed below. The OHCA shall enter into agreements with each such person in the time and manner required by law.

Name	Address/Contact/Phone	Function
Blue Cross Blue Shield of Louisiana	3501 N. Causeway Blvd. Suite 600 Metairie, LA 70002 Contact: Anne Dufour Telephone: 504.832.5843	Third Party Administrator
Blue Cross Blue Shield of Mississippi	Post Office Box 1043 Jackson, MS 39215-1043 Contact: Karen Martin Telephone: 601.664.4711	Third Party Administrator
Phelps Dunbar LLP	4270 I-55 North Post Office Box 16114 Jackson, MS 39236-6114 Contact: Seale Pylate Telephone: 601.360.9342	Legal Benefits Counsel
Jones Walker LLP	201 St. Charles Avenue Suite 2100 New Orleans, LA 70170 Contact: Timothy Brechtel Telephone: 504.582.8000	Legal Benefits Counsel
John Fayard Records Management and Storage	13486 Fastway Lane Gulfport, MS 39503 Telephone: 228.864.2262	Storage Facility
Iron Mountain	900 Distributors Row New Orleans, LA 70123 Contact: Robert Thornton Telephone: 504.818.1221	Storage Facility
Ace Data Storage, Inc.	3305 33rd Street, Suite A Gulfport, MS 39501 Contact: Cathy Fayard Facsimile: 228.864.6445	Storage Facility
Postlethwaite & Netterville	One Galleria Boulevard Suite 2100 Metairie, LA 70001 Contact: Ryan M. Berry Telephone: 504.837.5990	Auditor

Name	Address/Contact/Phone	Function
Discovery Benefits	4321 20th Ave S Fargo, ND 58103 Telephone: 877.765.8810	COBRA Administrator and Third Party Administrator for Health Care Spending Accounts
Benefitfocus	100 Benefitfocus Way Charleston, SC 29492 Contact: Christine Graham Telephone: 843.284.1052	Provides software support and hosting services
The Ultimate Software Group, Inc.	2000 Ultimate Way Weston, FL 33326 (954) 331-7023	Provides software support and hosting services
Mayo Foundation for Medical Education and Research	200 1st Street SW Rochester, MN 55905	Executive physicals
American Behavioral	3680 Grandview Parkway Suite 100 Birmingham, AL 35243 Contact: Deborah Garvin Telephone: 205.868.9633	EAP
Mercer	701 Poydras Street Suite 4125 New Orleans, LA 70139 Contact: Mimi Farrell Telephone: 504.571.2270	Insurance broker

HANCOCK HOLDING COMPANY AND SUBSIDIARIES

HIPAA SECURITY POLICIES AND PROCEDURES

EXHIBIT C

HIPAA Security Official's Job Description

When To Use:	When determining who should be the HIPAA Security Official; when training the HIPAA Security Official; when hiring your HIPAA Security Official.
Comments:	This is hereby incorporated into the Plan Sponsor's existing job description database.

Position Title: Hancock Holding Company OHCA HIPAA Security Official

General Description: Hancock Holding Company OHCA's HIPAA Security Official is an employee of **the Plan Sponsor** and is considered part of the **OHCA's** Plan Sponsor workforce. The HIPAA Security Official is responsible for overseeing the **OHCA's** activities relating to its development and implementation of the OHCA's HIPAA Security Policies and Procedures to ensure the confidentiality, integrity and availability of Electronic Protected Health Information as set forth in the federal Security Rule. The HIPAA Security Official is also responsible for overseeing the **OHCA's** maintenance of, and adherence, to these HIPAA Security Policies and Procedures.

Responsibilities:

- Take a lead role and assist in the formation, implementation, and maintenance of **the OHCA's** HIPAA Security Policies and Procedures.
- Maintain and ensure proper distribution of **OHCA's** HIPAA Security Policies and Procedures.
- Perform an assessment, with input from the various departments and employees, to identify, categorize and quantify security risks to Electronic Protected Health Information and to review the measures currently in place to address such security risks.
- Coordinate with **Hancock Holding Company's** legal counsel to ensure ongoing compliance with the HIPAA Security Rule and any applicable state laws.
- Perform or supervise the delivery of security training to the **OHCA** Plan Sponsor workforce.
- Assist in drafting appropriate Business Associate Agreement provisions; identifying Business Associate service providers; and developing appropriate monitoring under the HIPAA Security Rule of Business Associate arrangements.
- Establish and administer a system for receiving, documenting, tracking, investigating, and taking action on all complaints concerning **OHCA's** HIPAA Security Policies and Procedures or compliance with the HIPAA Security Rule.

- Consult with the Security Contact on matters regarding HIPAA Security compliance.
- Monitor legal changes and advancements in technology to ensure continued compliance.
- Maintain (or supervise the maintenance of) all documentation required by the HIPAA Security Rule.
- Recommend sanctions for failure to comply with the **OHCA's** HIPAA Security Policies and Procedures to the Chief Information Security Officer, who will consult with Human Resources to determine appropriate sanctions, if any.
- Cooperate with the U.S. Department of Health and Human Services, Office of Civil Rights, other legal entities, and **Hancock Holding Company's** legal counsel in any compliance reviews or investigations.
- Be the key contact and information source for all issues or questions relating to **OHCA's** compliance with the HIPAA Security Rule.

Qualifications:

- Knowledge of the HIPAA Security Rule.
- Understanding of HIPAA Security Rule as applied to group health plans.

HANCOCK HOLDING COMPANY AND SUBSIDIARIES

HIPAA SECURITY POLICIES AND PROCEDURES

EXHIBIT D

Policy and Procedures for HIPAA Security Training

When To Use:	Incorporate into existing company policies and procedures. Use to train relevant staff on security requirements.
Comments:	These policies and procedures for the HIPAA Security Training are not meant to be a stand-alone document. Incorporate into your HIPAA Security Policies and Procedures.

POLICY: Security Training

Employees of the Plan Sponsor who are considered part of the OHCA's Plan Sponsor "workforce" will be trained to understand and implement the OHCA's HIPAA Security Policies and Procedures and the HIPAA Security Rule.

PROCEDURES:

1. **The Hancock Holding Company Information Systems Security Officer as the HIPAA Security Official** has responsibility for implementation of this policy.
2. Timing of training.
   a. Upon the HIPAA Security Rule's initial compliance deadline.
   b. Within a reasonable time after becoming a workforce member of the "Plan Sponsor" under the HIPAA Security Rule.
   c. Within a reasonable time after material changes to **the OHCA's** HIPAA Security Policies and Procedures.
   d. Whenever, in the determination of **HIPAA Security Official**, additional training is necessary to ensure compliance with **OHCA's** HIPAA Security Policies and Procedures or the HIPAA Security Rule.
3. Training responsibility. The **HIPAA Security Official** is responsible for conducting the security training, or delegating the security training to an appropriately qualified employee or consultant.
4. Content of training. All employees will be trained in the following areas:
   a. At the determination of **HIPAA Security Official**, on all of **OHCA's** HIPAA Security Policies and Procedures, or, if appropriate, relevant policies and procedures for any particular employee if his or her job responsibilities do not necessitate training in all of the HIPAA Security Policies and Procedures;
   b. The administrative, physical and technical safeguards implemented by the Plan Sponsor to secure the confidentiality, integrity and availability of Electronic Protected Health Information;

c. Relevant provisions of the HIPAA Security Rule; and

d. The requirement that all employees report any Security Incidents, whether caused by a workforce member or a Business Associate, to **HIPAA Security Official or HIPAA Security Contact**.

5. Documentation. **The HIPAA Security Official** or his/her **HIPAA Security Contact** designee will maintain records indicating who has been trained, what training occurred, and the date of training, for six years following the date of the training. These documents will be maintained in the **Human Resources Department** or physically maintained by a Business Associate engaged for storage services.

HANCOCK HOLDING COMPANY AND SUBSIDIARIES

HIPAA SECURITY POLICIES AND PROCEDURES

EXHIBIT E

Policy and Procedures for HIPAA Security Contact

Comments: This is incorporated into existing Hancock Holding Company HIPAA Security Policies and Procedures and is used to train all staff on HIPAA security requirements.

POLICY: HIPAA Security Contact

OHCA's HIPAA Security Contact is the Sr. Tech Risk Mgmt Officer. The HIPAA Security Contact is responsible for assisting the HIPAA Security Official in responding to complaints and addressing Security Incidents. In addition, the HIPAA Security Contact administers several of the Plan Sponsor's policies regarding information security. Given the scope, such policies also apply to electronic PHI.

PROCEDURES:

1. The **HIPAA Security Contact** will promptly forward all information regarding Security Incidents when received to the **HIPAA Security Official.**

2. Documentation. **OHCA**'s HIPAA Security Contact designations will be maintained by **the Human Resources Department** (but may be physically stored with a Business Associate) for six years following the year a person ceased to serve in that position.

HANCOCK HOLDING COMPANY AND SUBSIDIARIES

HIPAA SECURITY POLICIES AND PROCEDURES

EXHIBIT F

Policy and Procedures for Security Incidents

When To Use:	Incorporate into existing company policies and procedures. Use to train all staff on HIPAA security requirements.
Comments:	The Policy and Procedures for Security Incidents are not meant to be a stand alone document. You should incorporate it into your HIPAA Security Policies and Procedures.

POLICY: Security Incidents

The Hancock Holding Company OHCA's HIPAA Security Contact and HIPAA Security Official will receive and respond to complaints and information regarding Security Incidents.

PROCEDURES:

1. **HIPAA Security Official** has responsibility for implementation of this policy.

2. **If HIPAA Security Contact and HIPAA Security Official are different**: **HIPAA Security Contact** will forward all information regarding the Security Incident to **HIPAA Security Official**.

3. Upon receiving notice of a Security Incident, **HIPAA Security Official** will investigate and, with the assistance of **its legal counsel** if necessary, determine the necessary response.

4. If the HIPAA Security Official determines that the Security Incident actually occurred, the following steps will be taken:

    a. Determine whether there is any harm that should be mitigated, if practicable;

    b. If the violation was by the Plan Sponsor's workforce member, consider whether sanctions should be imposed;

    c. If the violation was by a Business Associate, determine whether further investigation or actions are necessary to ensure future violations do not occur;

    d. Consider, in light of the nature of the violation, if additional training should occur for one or more employees; and

    e. Consider, in light of the nature of the violation, whether any HIPAA Security Policies or Procedures need to be amended.

5. Documentation. **HIPAA Security Official** will maintain all records relating to Security Incidents and their resolution for six years following the date the Security Incident was resolved. These documents will be maintained in the **Human Resources Department** or physically maintained by a Business Associate engaged for storage services.

HANCOCK HOLDING COMPANY AND SUBSIDIARIES
HIPAA SECURITY POLICIES AND PROCEDURES

ADDENDUM
IT Department Necessary Employees Designations

In addition to the Necessary Employees identified in Exhibit B of these Security Policies and Procedures, the following associates who are members of the IT Department have been designated as Necessary Employees:

Name/Title	**Functions/Limitations**
Bus Systems Analyst Sr	Supports Business Systems
Database Administrator	Supports/Maintains Server Databases
Desktop Support Spec	Supports/Maintains Workstations
Dir – Info Tech Svcs	Manages Information technology Associates, and has access to Servers
Info Security Analyst 1	Supports Information Security Initiatives; Access to Servers
Info Security Analyst 2	Supports Information Security Initiatives; Access to Servers
Info Security Analyst 3	Supports Information Security Initiatives; Access to Servers
Info Security Team Lead	Supports Information Security Initiatives; Access to Servers
IT Service Analyst 1	Access to Servers as part of support duties
IT Service Analyst 2	Access to Servers as part of support duties
Mgr – Database Admin	Supports/Maintains Server Databases
Mgr – Desktop Service	Supports/Maintains Workstations
Mgr – Distributed Systems	Supports/Maintains Servers
MGR – Enterprise Storage	Supports/Maintains Enterprise Storage

Name/Title	Functions/Limitations
Mgr – Info Security	Information Security – Access to Servers
Mgr – Info Services	Information Data Services – Access to Servers
Mgr – LAN Administration	Supports/Maintains Servers/Workstations
Mgr – Network Services	Supports/Maintains Network – Access to Servers
Network Engineer 1	Supports/Maintains Network – Access to Servers
Network Engineer 2	Supports/Maintains Network – Access to Servers
Network Voice Integrator	Supports/Maintains Network – Access to Servers
Service Desk Analyst	Supports Service Desk – Analyze Initial Requests
Spvr – Remote Market	Supports/Maintains Servers/Workstations
Sr. Desktop Support Spec	Supports/Maintains Workstations
Sr Tech Risk Mgmt Ofcr	IT Compliance – Access to Servers
Sr Tech Analyst – TL	Supports/Maintains Servers/Workstations
Sr Technical Analyst	Supports/Maintains Servers/Workstations
Storage Administrator	Supports/Maintains Enterprise Storage
Technical Analyst	Supports Technology Initiatives

The titles set forth above are current as of June 15, 2014. The IT Department will review this list annually and update the designation of Necessary Employees as needed after consultation with the Security Officer. However, any change in the above titles that does not impact a Necessary Employee's need to access PHI and/or e-PHI to perform his or her job duties will be deemed to be incorporated based on his or her original designation as a Necessary Employee.

Without limiting the above list of Necessary Employees, any associate who is a member of the following Active Directory Groups may have access to e-PHI by virtue of their job duties to control server and workstation security and access:

Server Admins	Central Computing	WKS Admin
System Admins	Sql-Systems Admin	Domain Admin

HANCOCK HOLDING COMPANY AND SUBSIDIARIES
ORGANIZED HEALTH CARE ARRANGEMENT

HIPAA SECURITY POLICIES AND PROCEDURES

ACKNOWLEDGEMENT

By execution below, I acknowledge that I have read the Hancock Holding Company and Subsidiaries Organized Health Care Arrangement HIPAA Security Policies and Procedures. I understand that effective as of September 23, 2013 these Security Policies and Procedures have been amended and restated in their entirety and that as a Necessary Employee, I may have access to Electronic Protected Health Information. I agree to comply with these HIPAA Security Policies and Procedures and understand that compliance with these policies and procedures is a condition of my employment. I acknowledge that the Manager – Information Security is the Security Official and the Sr. Tech Risk Mgmt Officer is the Security Contact and that I have been given the opportunity to ask questions about these HIPAA Security Policies and Procedures.

_____ _____

Signature Date

_____

Print Name

Retain these HIPAA Security Policies and Procedures and return this acknowledgement to the Security Contact.