

ONE HEALTH QUALITY ALLIANCE, LLC HIPAA POLICY AND PROCEDURES

Adventist Healthcare, Inc. and various participating physicians (the "Members") have formed a clinically integrated network, One Health Quality Alliance, LLC, a Maryland limited liability company ("OHQA") to develop and implement procompetitive and beneficial opportunities to improve quality in the provision of health services, improve population health, improve access to healthcare services and reduce health care costs and to offer new and innovated products, services or arrangements, including governmental or commercial third party payer products as well as any other business or activity that is necessary and proper to accomplish the purposes of OHQA. To accomplish procompetitive and beneficial opportunities as just described, discussions and information exchanges among the Members through their employees and others with OHQA will be necessary. As a part of these discussions and information exchanges, it is possible that patient contact may occur or the Members may need to furnish or cause to be furnished to OHQA or each other protected health information subject to the Health Insurance Portability and Accountability Act ("HIPAA") and regulations issued pursuant thereto, both as amended from time-to-time.

A. Statement of Purpose

The purpose of this HIPAA Policy ("Policy") is to enunciate and detail OHQA's commitment to adhere to the Health Insurance Portability and Accountability Act and regulations issued pursuant thereto, both as amended from time-to-time. It is OHQA's policy to establish standard processes and guidelines for addressing adherence to HIPAA.

B. General HIPAA Compliance Policy and Scope

It is the policy of the OHQA that the OHQA and the activities of its employees, agent and Members shall comply in every way with the requirements of HIPAA. Therefore, the OHQA is adopting the following procedures and guidelines to which the OHQA intends to adhere and which it expects all of its employees, agents, and Members to adhere with respect to all activities for the OHQA as defined below.

The Members, OHQA and its Board of Directors ("Board"), employees and agents in its management of the OHQA's business and affairs shall be committed to adhere to HIPAA in all OHQA activities, as well as all other laws applicable to the business and affairs of the OHQA. In furtherance of this responsibility, the Board shall establish policies and procedures governing the operations of the OHQA and that of its Members, employees, and agents, as defined below, when engaged in OHQA activities, as defined below, to establish and maintain HIPAA compliance.

OHQA and its Members shall distribute this Policy or otherwise make it known to, and shall ensure the compliance of, all of their relevant employees, and agents engaged in OHQA activities.

Business Associate Agreements or Other Agreements. With respect to the activities of OHQA Projects, as defined in the OHQA Operating Agreement, OHQA and its Members shall abide by the terms and conditions of any Business Associate Agreement (“BAA”) (as that term is defined in HIPAA) or other HIPAA required agreement with regard to the activities of OHQA, as well as this Policy, the intent of which is to establish or ensure that the OHQA comply with HIPAA. Guidelines for the contents of a BAA are set forth in Section V of this Policy.

C. Definitions

As used in this Policy, the following terms have the following meanings:

“Staff” means a person who is an OHQA employee, agent or a Member’s hospitals, physicians, directors, officers, management staff, employees and any other persons acting through on behalf of OHQA on an OHQA Project which requires HIPAA compliance.

All capitalized terms not defined in this Policy are defined in OHQA’s Operating Agreement.

I. PATIENT'S RIGHTS

It is the policy of the OHQA to provide patients of Members or their subsidiaries all the rights enumerated under HIPAA applicable to OHQA in its activities on behalf of its Members.

II. COMPLIANCE POLICY

OHQA, its employees and agents and OHQA’s Members, and their directors, officers, and employees as well as any other persons acting through on behalf of OHQA have a long standing commitment to protect the privacy of patient health information which is sometimes referred to as Protected Health Information (“PHI”). A part of this commitment is to be compliant with the privacy standards contained in the regulations promulgated under HIPAA. OHQA may use PHI for purposes of evaluation of treatment, payment and health care operations. OHQA may disclose PHI (i) with the individual patient’s authorization; (ii) to Covered Entities or Business Associates in compliance with HIPAA regulations; and (iii) in certain other circumstances as permitted in compliance with HIPAA regulations, including through the service of a subpoena or other judicial request. In using or disclosing PHI, OHQA shall restrict use or disclosure to the minimum amount of PHI necessary to accomplish the purpose of use or disclosure. OHQA shall respect the rights of the individual regarding his or her PHI. OHQA shall develop and implement safeguards to protect PHI.

In order to assure compliance, OHQA will performed risk assessments, outlined below, to insure that the number of persons who have access to PHI through OHQA is limited. All appropriate OHQA staff are required to complete HIPAA training through an OHQA Member on an annual basis. In addition, all appropriate OHQA staff shall be made aware of OHQA specific HIPAA protocols contained in this document. OHQA shall document its efforts to achieve compliance. OHQA’s legal counsel, Baudino Law Group, PLC shall be its Designated Privacy Official.

PROCEDURE:

Permitted Uses & Disclosures by OHQA Staff:

OHQA may utilize PHI for evaluation of health care operations as well as for treatment and payment evaluation. PHI is utilized by OHQA staff on a need-to-know basis.

Risk Assessment:

An assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic PHI will be performed annually utilizing Chapter 6 of the ONC's Guide how to complete a risk assessment *Guide to Privacy and Security of Electronic Health Information* with the results reported to OHQA's Board.

Physical Access to PHI:

- (1) All OHQA staff will make every effort to conceal or screen paper charts, records, faxes, or other documentation containing PHI from unauthorized individuals. Verbal communication shall be conducted in the most discreet manner possible.
- (2) Computer printouts, faxes, records, reports, and other paper records shall not be left in open work areas so as to expose the contents of the records. Files and papers shall be put away when not in use.
- (3) OHQA staff shall take precautions to ensure that PHI may not be viewed by unauthorized individuals from equipment, including workstations, fax machines, copiers, and printers (methods include but are not limited to use of screen savers, timeouts, etc.).
- (4) The display screens for all personal computers, workstations, and terminals must be positioned such that they cannot be easily viewed through a window, by persons walking in a hallway, or by individuals in public areas.
- (5) Fax machines and printers used to print PHI must be located in such a manner that the printouts cannot be readily viewed through a window, by persons walking in a hallway, or by individuals in other public areas.
- (6) OHQA employees who work on laptop computers and with paper medical records or documents should be aware of their surroundings with regard to unauthorized viewing of PHI.
- (7) OHQA employees should not transmit PHI to any type of alpha paging device.
- (8) File cabinets should be locked when not properly supervised.

- (9) Faxes, computer printouts, and copies/originals should be collected as soon as possible and appropriately filed.
- (10) Any offices of OHQA shall be locked whenever at least one OHQA staff member is not on site.
- (11) OHQA staff shall set up password protection on all personal computers on which PHI is stored, maintained, or transmitted.
- (12) When the employment or other arrangement of OHQA workforce member ends, all access to electronic PHI shall be terminated immediately.

Faxing of PHI:

- (1) Except for purposes of treatment, payment or operations, faxing of PHI is limited to instances where time is a critical factor.
- (2) The recipient's fax number should be verified prior to transmission.
- (3) A cover sheet with a statement regarding confidentiality shall be included on the cover page of the transmission.

Transmitting of PHI via E-Mail, US Mail, Courier Service, or Hand Delivery:

- (1) All transmissions of PHI must be documented by the Designated Privacy Official.
- (2) All transmissions of PHI to subcontractors require the execution of a Business Associate Agreement to obtain satisfactory assurances that the subcontractor will appropriately safeguard the PHI administratively, physically and technically.

Handling Confidential Information in Meetings:

- (1) Meetings where PHI is discussed are to be attended by individuals (including employees, physician members, hospital representatives, managed care payor representatives, etc.) who have been specifically invited, or by individuals with a specific business purpose for attending. These meetings are to be conducted in a secure area, such that PHI is not overheard or viewed by unauthorized personnel.
- (2) All meetings with third party visitors who are not authorized to have access to PHI must take place in a fully enclosed conference room or office, if workers in the immediate area of the meeting room are handling PHI.
- (3) When PHI has been recorded on black boards or white boards, it must be erased before the authorized recipients of this information leave the area.

- (4) If documents containing PHI are distributed during the course of the meeting, and those documents are not required by the recipient for health care operations, the documents must be collected and destroyed at the completion of the meeting.
- (5) A confidentiality statement is to be on the agenda of all meetings that deal with PHI. A sample is as follows: “The purpose of the _____ Committee / Meeting is to enhance quality care delivery within the OHQA. As such, all discussions, records, and reports of the Committee pursuant to its purpose are considered to be strictly confidential and entitled to all protection provided by law.”

Release of PHI:

- (1) Should OHQA staff have a reason to release PHI for reasons other than treatment, payment, or health care operations, OHQA staff shall not disclose PHI unless it first obtains a valid authorization from the patient or patient’s legally designated representative.
- (2) OHQA will restrict reproduction of PHI to assure patient privacy and rights as well as the integrity of the OHQA system.

Responding to a Subpoena Requesting PHI:

In addition to taking all protections allowable by applicable state or federal law, as applicable, while complying with subpoenas, court orders or other lawful requests for PHI, OHQA shall do the following:

- (1) If the subpoena or other lawful request is accompanied by an order of a court or administrative tribunal, OHQA will verify the identity and authority of the individuals requesting PHI.
- (2) If the order of the court or other administrative tribunal is valid and meets the verification requirements, OHQA will disclose only that PHI expressly authorized by such order.
- (3) If the subpoena, discovery request or other lawful process (“subpoena”) is not accompanied by a court order, OHQA will disclose the PHI only after obtaining satisfactory assurances from the party seeking the information that they have made reasonable efforts:
 - a. To notify the individual who is the subject of the requested PHI, or
 - b. To secure a qualified protective order.
- (4) Notice to Individual. Prior to disclosing PHI when the subpoena is not accompanied by a court order and there is no qualified protective order meeting

the requirements of the HIPAA privacy rules, OHQA will obtain a written statement and accompanying documentation from the requesting party that meets all of the following requirements:

- a. The written statement and documentation must demonstrate that reasonable efforts have been made to give notice of the request to the individual who is the subject of the requested PHI;
 - b. The notice must contain sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and
 - c. The written statement and accompanying documentation must demonstrate that:
 - i) Time for raising objections to the court or administrative tribunal has elapsed;
 - ii) No objections were filed; or
 - iii) The court has resolved all objections filed by the individual or the administrative tribunal and the disclosures being sought are consistent with such resolution.
- (5) Qualified Protective Order. A qualified protective order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
- a. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
 - b. Requires the return to OHQA or destruction of the PHI, (including all copies made) at the end of the litigation or proceeding.
- (6) Prior to disclosing PHI when the subpoena is not accompanied by a court order and the above notice requirements are not met, OHQA will obtain from the requesting party a written statement and accompanying documentation demonstrating that:
- a. The parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
 - b. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

- (7) If the requesting party is unable to meet the requirements for Notice or a Qualified Protective Order, OHQA will notify the requesting party that it is unable to comply with the subpoena.
- (8) If the requesting party decides to pursue the request for the PHI without meeting the above requirements, OHQA's Designated Privacy Official will contact OHQA's legal Counsel for further direction.
- (9) OHQA's Designated Privacy Official shall document the information regarding the subpoena or other legal process that requests PHI in an *Accounting of Disclosures* Log.
- (10) The subpoena and any documents produced for the subpoena will be retained according to state and federal regulations.

Breaches of PHI:

- (1) All suspected or known security incidents and their outcomes shall be documented.
- (2) All suspected or known security incidents shall be mitigated to the extent practicable
- (3) All suspected or known security incidents, including breaches of unsecured PHI, shall be reported as required by HIPAA as soon as practicable.
- (4) Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology specified by the Secretary, e.g. unencrypted.
- (5) All breaches of unsecured PHI involving more than 500 individuals shall require the notification of the print and broadcast media for the area as defined in HIPAA.
- (6) All breaches of unsecured PHI involving less than 500 individuals shall be documented on a log and within 60 days after the calendar year on the HHS website.

Destruction of PHI:

OHQA staff shall maintain PHI as long as is deemed necessary. Such PHI may be maintained in paper copy, on computer drives, or on diskettes. When OHQA staff feel it is no longer necessary to maintain PHI, such data shall be destroyed as follows: paper copies shall be shredded or incinerated, computer files shall be deleted, and diskettes shall be broken. Such data shall not be placed into trash bins until after it is destroyed as outlined above.

Sanctions:

- (1) When a concern arises regarding a possible violation of HIPAA or OHQA's policies or procedures related to HIPAA or PHI, the Designated Privacy Official shall begin an investigation promptly.
- (2) If, at the conclusion of the investigation, it is found that a violation of OHQA's policy or procedure has occurred, the employee involved shall be disciplined in accordance with the severity of the violation and any disciplinary policy of OHQA.
- (3) OHQA staff who fail to comply with these policies and procedures will have their violations classified according to intent as follows: (i) Level 1 - if the failure to comply was inadvertent and unintentional; and (ii) Level 2 - if the failure to comply was intentional or shows a purposeful disregard of OHQA policy.
- (4) The disciplinary action report documenting the OHQA staff person's violation shall be placed in the employee's personnel file and the Designated Privacy Official's files.

III. BREACH NOTIFICATION

A. Policy

It is the policy of OHQA to comply with the breach notification provisions established at 45 CFR 164.400. Under the regulations, "breach" means the acquisition, access, use, or disclosure of protected health information ("PHI") in a manner not permitted under the regulations which compromises security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed unless and until OHQA or Business Associate demonstrates through its risk assessment that there is a low probability that the PHI has been compromised. All notifications required under this Policy shall be made without unreasonable delay and in no case later than sixty (60) calendar days after discovery of a breach.

B. Guidelines

1. Breaches Do Not Include
 - a. A breach does not include any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access or use was made in good faith and within the scope of the individual's authority and does not result in further use or disclosure in a manner not otherwise permitted under the law.
 - b. A breach also does not include any inadvertent disclosure by a person who was authorized to access PHI at OHQA to another person authorized to access PHI at OHQA or organized health care arrangement in which OHQA participates, and the information was

received as a result of such disclosure is not further disclosed in a manner not permitted by law.

- c. Finally, a breach does not include a disclosure of PHI where OHQA has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. Procedure

- a. Any employee who discovers a suspected breach must immediately notify the Designated Privacy Officer. The employee may notify the Designated Privacy Officer of the occurrence of a suspected or potential breach in any format including in writing, electronically or orally. The Designated Privacy Officer will document the report of a potential breach, along with the date and time that they were notified of such event.
- b. As the Designated Privacy Officer is OHQA's legal counsel, if the potential breach involves PHI, legal counsel will review the matter to determine whether and how the potential breach should be reported. Legal counsel will also determine whether any additional notifications are required pursuant to applicable breach notification law.
- c. Legal counsel will conduct an initial review of the suspected breach to determine whether a breach occurred and, if so, the scope, magnitude and severity of the breach, mechanisms for mitigating the harmful effects of the breach, and ways to remediate the vulnerability that led to the breach.
- d. OHQA, in conducting its review, shall complete a four-factor risk assessment within a reasonable time after the discovery of the breach. The risk assessment shall include:
 - 1) The nature and extent of the PHI involved, including the type of identifiers and likelihood of re-identification.
 - 2) The identity of the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made. Did the recipient of the PHI have an independent obligation to protect the privacy and security of the PHI?
 - 3) Was the PHI actually acquired or viewed, or was there only an opportunity to do so?
 - 4) The extent to which the risk to the PHI was mitigated.

- e. The above factors must be considered and documented in a risk analysis to determine whether there is a low probability that the PHI was compromised. Unless there is a low probability that the PHI was compromised a breach notification is required.
- f. If the review shows that no breach has occurred, or that a low probability of PHI being compromised, the Designated Privacy Officer will document this in a report, along with all other information that supports such conclusions and no further investigations and procedures are required.
- g. If the review shows that a breach has occurred, notification will be made to the individual in accordance with the requirements of 45 CFR 164.404.
 - 1) Notify each individual whose unsecured PHI has been breached within sixty (60) calendar days of discovery of the breach.
 - 2) The notification shall include the following:
 - a) Date of the breach, date of discovery and a brief description of what occurred;
 - b) Description of the type of unsecured PHI involved in the breach;
 - c) Steps to be taken to mitigate potential harm;
 - d) Description of what OHQA is doing to investigate, mitigate and protect against future breaches;
 - e) Contact information so that the patient whose PHI was breached, or his/her authorized representative may request information from OHQA.
 - 3) The notice should be in writing by first class mail, return receipt requested to the last known address, or if the individual agrees, electronically. In limited circumstances an individual may opt for privacy reasons to receive communication from OHQA orally or by telephone. In those instances OHQA should request the individual pick up the written notice of the breach.

- h. For breaches of unsecured PHI involving less than 500 individuals, OHQA shall maintain a log or other documentation of such breaches and not later than sixty (60) days after the end of each calendar year in which the breaches were discovered, notify the Secretary of HHS.
- i. If the breach involves unsecured PHI involving more than 500 individuals, OHQA shall notify a media outlet serving in the State, and shall also notify the Secretary of HHS of such breach.

IV. BUSINESS ASSOCIATE AGREEMENTS

A. Policy

It is the policy of OHQA that for any person or entity that performs services on behalf of OHQA, for which person or entity receives or uses protected health information ("PHI"), a Business Associate Agreement ("BAA") must be obtained. A "Business Associate" is any person or organization that performs, or helps to perform, any function or activity that involves the use or disclosure of PHI on behalf of OHQA, including but not limited to claims processing or administration; utilization management; benefit management; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services; and patient safety activities. PHI may be disclosed to a business associate only if OHQA receives satisfactory assurances in writing that the business associate will safeguard the privacy of the PHI that it creates and oversees.

B. Guidelines for a BAA

1. Business Associates include subcontractors that create, receive, maintain or transmit PHI on behalf of the Business Associate;
2. Written contracts or agreements must be negotiated between OHQA and any Business Associate that will handle PHI;
3. Business Associate Agreements shall include provisions which:
 - a. Identifies the uses and disclosure of PHI permitted under the contract;
 - b. Allows the Business Associate to use or disclose the PHI only as permitted under these privacy standards;
 - c. Restricts use and disclosure of the PHI that the Business Associate creates or receives to those that are specified in the contract;
 - d. Requires the Business Associate to establish safeguards to prevent use and disclosure other than as provided for in the contract with OHQA;

- e. Provide for reporting to OHQA of any use or disclosure of PHI not provided for under the Business Associate's contract;
6. Requires the Business Associate to apply the same restrictions and conditions on use and disclosure of PHI to the agents and subcontractors to whom it forwards the PHI. The Business Associate Agreement should require the Business Associate to obtain satisfactory assurance in the form of a Business Associate Agreement from their subcontractor business associate;
 7. Makes PHI available to patients as provided under patient access to health information;
 8. Amends any PHI it receives when asked to so by OHQA;
 9. Makes available to OHQA the information it needs to account for the uses and disclosures of PHI as provided for under the accounting for disclosures;
 10. A written provision requiring the Business Associate that is aware of noncompliance by its subcontractors must respond to situation as OHQA would (i.e., by trying to cure the breach, ending the violation or terminating the contract);
 11. The Business Associate Agreement will require the Business Associate:
 - a. Where applicable, comply with the security rule with respect to electronic PHI;
 - b. To report breaches of unsecured PHI as required by the breach notification rule;
 - c. To ensure that any subcontractor that creates, receives, maintains or transmits PHI on behalf of the Business Associate agree to the same restrictions that apply to the Business Associate;
 - d. That to the extent that Business Associate is to carry out the covered entity's obligation under the privacy rule, the Business Associate comply with the requirements of the privacy rule that apply to OHQA in the performance of such obligation.
 12. Makes internal practices and its records related to the use and disclosure of PHI available to the U.S. Department of Health and Humans Services for purposes of determining compliance with the privacy standards;

13. Returns, if feasible, PHI to OHQA upon termination of the contract or destroys any copies of such information pursuant to one of the destruction methods provided by law. If return and destruction of PHI is not feasible, the Business Associate must extend contractual protection for the use and disclosure of the information for purposes that make its return and destruction not feasible; and
14. Provides for possible termination of the underlying contract with the Business Associate if Business Associate violates the contractual provisions.

Evaluation:

These HIPAA Policies and Procedures shall be evaluated every two (2) years, or as required by HIPAA regulations.

Information System Activity Review *A regular audit and review of the records of information system activity such as audit logs, access reports and security incident tracking reports will be performed based on the OHQA Information System Activity Review – See, 45 CFR 164.308(a)(1)(ii)(D);*

Data Backup Plan *will be instituted to create and maintain retrievable exact copies of EPHI in accordance with the OHQA Data Backup Plan. See, 45CFR 164.308(a)(7)(ii)(A);*

Disaster Recovery Plan *will be implemented to restore any loss of data following the OHQA Disaster Recovery Plan. – See, 45 CFR 164.308(a)(7)(ii)(b);*

Emergency Mode Operation Plan *- A plan to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode will be implemented following OHQA Emergency Mode Operation Plan. See, 45 CFR 164.308(a)(7)(ii)(C).*

Designated Privacy Official:

OHQA's Designated Privacy Official is: Arumani Manisundaram.

Adopted May 27, 2015

ONE HEALTH QUALITY ALLIANCE, LLC

By: 

Name: STEVEN L. TUCK, M.D.

Title: CHAIR