

April 19, 2005

IMPORTANT - QHA CUSTOMERS AND VENDORS - HIPAA UPDATE!!!

HIPAA Administrative Simplification

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

It also addresses the security and privacy of health data. Potentially, adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

Health Insurance Portability and Accountability Act (HIPAA) Security Rule - APRIL 20, 2005

As you may be well aware of the law, the implementation date for the Health Insurance Portability and Accountability Act (HIPAA) Security Rule is April 20, 2005. The Security Rule requires all covered entities to evaluate procedures and adopt certain security measures to protect electronic protected health information (ePHI).

The HIPAA Security Rule defines a security incident as "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with system operations in an information system." 45 C.F.R. 164.304

In general, the Privacy (April 2004) and Security Ruling (April 20, 2005) requires a Business Associate (QHA) receiving Electronic Protected Health Information (ePHI) to:

- a) Not use or disclose PHI other than as permitted by the agreement or required by law
- b) Use appropriate safeguards to protect the confidentiality of the information
- c) Report to the covered entity any use or disclosure not permitted by the agreement
- d) Ensure agreement by any agents or subcontractors to the same restrictions and conditions as the business associate
- e) Make available to the covered entity the information as necessary for it to comply with the patients' rights to access, amend and receive an accounting of disclosures of their PHI
- f) Make available to the Secretary of the Department of Health and Human Services (DHHS) the business associate's internal practices, books and records relating to the use and disclosure of PHI
- g) Return or destroy the information once the contract is terminated, if feasible

It is the belief, and opinion, of Quantum Health Automation (QHA) that the QHA Business Associate Agreement (BAA) currently in place with our provider offices - as of

a result of the Privacy Rule implementation April 2004 - is consistent with the Security Rule and need not any revisions to the existing contract. At this time, QHA does not deem necessary any addendums to achieve HIPAA compliancy.

In particular, and listed below, the Security ruling assumes the following obligations regarding electronic Protected Health Information (ePHI).

In addition to the points of reference below, QHA has stamped actual and current segments of the QHA Business Associate Agreement (BAA) to address and identify QHA's obligations as a Business Associate of the Security Rule. QHA's BAA specifies clearly throughout the current contract "Required by Law". For purposes of interpreting legal meaning below, and as defined in the QHA Business Associate Agreement, the definition of "Required by Law" shall have the same meaning as the term required by law in 45 CFR & 164.501 (of the HIPAA regulations).

Ruling I:

Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI that it creates, receives, maintains or transmits on behalf of the Covered Entity in accordance with 45 CFR 164 (the HIPAA Security Rule).

QHA BAA:

3.) Business Associate hereby agrees to maintain the security and privacy of all protected health information in a manner consistent with Indiana and federal laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Regulations thereunder, and all other applicable law.

6.) Business Associate shall not disclose protected health information created or received by Business Associate on behalf of Customer to a person, including any agent or subcontractor of Business Associate but not including a member of Business Associate's own workforce, until such person agrees in writing to be bound by the provisions of this Agreement and applicable Indiana or Federal law.

7.) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of protected health information not permitted by this Agreement or applicable law.

Ruling II:

Business Associate will ensure that any agent, including a subcontractor, to whom it provides e-PHI that was created, received, maintained or transmitted on behalf of the Covered Entity agrees to implement reasonable and appropriate safeguards to protect the ePHI.

QHA BAA:

1.1 Moreover, Business Associate may disclose Protected Health Information for the purposes authorized by this Agreement including, but not limited to, Section 1.2 below and Section 5 and 6 of this Agreement below.

- (i) to its employees; and
- (ii) subcontractors and agents
- (iii) as directed by the Customer

1.2 Business Associate may use and disclose Protected Health Information for the proper management and administration of the Business Associate, as provided in Business Associate's then said Electronic Claims and Transaction Service Agreement; and to provide data aggregation/analysis services relating to the health care operations of the Customer.

5.) Business Associate shall not disclose protected health information to any member of its workforce unless Business Associate has advised such person of Business Associate's privacy and security obligations under this Agreement, including the consequences for violation of such obligations. Business Associate shall take appropriate disciplinary action against any member of its workforce who uses or discloses protected health information in violations of this Agreement and applicable law.

6.) Business Associate shall not disclose protected health information created or received by Business Associate on behalf of Customer to a person, including any agent or subcontractor of Business Associate but not including a member of Business Associate's own workforce, until such person agrees in writing to be bound by the provisions of this Agreement and applicable Indiana or Federal law.

Ruling III:

Business Associate agrees to alert Covered Entity of any security incident (as defined by the HIPAA Security Rule) of which it becomes aware.

QHA BAA:

9.) Business Associate agrees to report to Customer any unauthorized use or disclosure of protected health information by Business Associate or its workforce or subcontractors and the remedial action taken or proposed to be taken with respect to such use or disclosure.

Ruling IV:

Business Associate authorizes termination of the Business Associate Agreement if the Covered Entity reasonably determines that Business Associate has violated the Security Rule.

QHA BAA:

13.) In the event Business Associate or Customer fails to perform the obligations under this Agreement, Customer or Business Associate may, at its option:

a) Require Business Associate or Customer to submit to a plan of compliance, including monitoring by Customer or Business Associate and reporting by Business Associate or Customer, as Customer or Business Associate, in its sole discretion, determines necessary to maintain compliance with this Agreement and applicable law. Such plan shall be incorporated into this Agreement by amendment hereto; and

b) Business Associate agrees to mitigate, to the extent reasonably practicable, any harmful effect, that is known to Business Associate, of a use or disclosure of PHI by Business Associate in violation of this Agreement.

c) Immediately discontinue providing protected health information to Business Associate with or without written notice to Business Associate.

14.) Customer or Business Associate may immediately terminate this Agreement and related agreements if Customer or Business Associate determines that the Business Associate or Customer has breached a material term of this Agreement. Alternatively, Customer or Business Associate may choose to:

(i) provide Business Associate or Customer with ten (10) days written notice of the existence of an alleged material breach; and (ii) afford the Business Associate or Customer an opportunity to cure said alleged material breach to the satisfaction of Customer or Business Associate within ten (10) days. The Business Associate's or Customer's failure to cure shall be grounds for immediate determination of this Agreement. Customer's and Business Associate's remedies under this Agreement are cumulative, and the exercise of any remedy shall not preclude the exercise of any other.

15.) Upon termination of this Agreement, Business Associate shall return or destroy all protected health information received from Customer, or created or received by Business Associate on behalf of Customer and that Business Associate maintains in any form, and shall retain no copies of such information. If the parties mutually agree that return or destruction of protected health information is not feasible, Business Associate shall continue to maintain the security and privacy of such protected health information in a manner consistent with the obligations of this Agreement and as required by applicable law, and shall limit further use of the information to those purposes that make the return or destruction of the information infeasible. The duties hereunder to maintain the security and privacy of protected health information shall survive the discontinuance of this Agreement.

QHA has created in-house data policies and protocols to effectively maintain the privacy, confidentiality and security of data transmitted/received, as the HIPAA Privacy &

Security Guidelines have established - under which - protected health information (ePHI) may be used by entities (providers, clearinghouses and payers).

QHA is continuing to implement authentication and encryption measures deemed "appropriate and reasonable" for data activities within the entire provider-to-clearinghouse-to-payer framework crucial to ensuring data privacy, confidentiality and security.

QHA is committed to ensuring its customers that data will be secure, protected and maintained set forth by HIPAA Privacy and Security Rulings.

Because providers have placed such trust in QHA, with highest expectations of data privacy and security, QHA wants to inform our customers in detail of our daily practices in protecting our customers' interest both now, and in the future.

Regards,

QHA HIPAA Support
201 NW Fourth Street, Ste 103
Evansville, Indiana 47708
hipaa@qhaclaims.com
www.qhaclaims.com
800-500-8747 Toll Free
812-468-8477 Local
812-468-8478 Fax

The contents of this statement are intended for general informational and educational purposes only and should not be construed as legal advice. The information is not intended to create, nor does its receipt constitute, an attorney-client relationship. Readers are urged not to act upon the information contained in this statement without first consulting an attorney licensed in the appropriate jurisdiction. This statement is prepared as a service to QHA customers and is believed by Quantum Health Automation (QHA) to be reliable. QHA cannot control or provide any warranty about the content, availability, or accuracy of the information contained on any referenced internal or external source.