Last Updated October 2013

HIPAA Readiness Disclosure Statement

HealthLink has been following the evolution of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) since its inception in 1996. Our goal is to help ensure that our systems, supporting business processes, policies, and procedures successfully meet the implementation standards and deadlines mandated by the United States Department of Health and Human Services.

HIPAA Applicability

HIPAA Title II, sometimes called Administrative Simplification, has two primary areas of regulation: (1) the standardization of certain electronic health care related transactions, and (2) the implementation of controls to protect an individual's health information.

The HIPAA Administrative Simplification rules and regulations apply to covered entities defined as health plans, health care clearinghouses and health care providers who transmit any health information electronically in transactions covered under the rules, and who receive, maintain or disclose individually identifiable health information in any form or medium. All covered entities must comply with the standards adopted by HIPAA by the applicable compliance dates.

HIPAA Privacy and Security Rules

Privacy

Compliance Required and Achieved April 14, 2003

HealthLink complied with the provisions of the HIPAA Privacy Rule by the required date of April 14, 2003. Compliance efforts included, but were not limited to:

- appointing a Privacy Officer,
- establishing a Privacy Office
- creating an infrastructure to support ongoing compliance requirements throughout the company, including adopting and communicating policies, standards and procedures, and training all associates each year.

HealthLink has adopted policies and procedures that comply with the HIPAA Privacy regulation, including granting the following individual rights:

- An individual's right to access his or her designated record set containing his or her own protected health information (PHI).
- The right to request an amendment to PHI contained in a designated record set.
- The right to request a restriction on the use and disclosure of PHI for treatment, payment and health care operations.
- The right to authorize the use of protected health information before its use in certain marketing activities.
- The right to receive confidential communications at an alternate address or location.
- The right to request an accounting of certain disclosures.
- The right to voice a complaint pertaining HealthLink's privacy policies and procedures.

Privacy notices describing the company's use and disclosure of PHI are distributed to all fully insured subscribers.

Security

Compliance Required and Achieved April 20, 2005

HealthLink complied with the provisions of the HIPAA Security Rule by the required date of April 20, 2005. Compliance efforts included, but were not limited to:

- appointing a Corporate Information Security Officer
- establishing an Information Security Compliance Office
- creating an infrastructure to support ongoing compliance requirements throughout the company including adopting and communicating policies, standards and procedures, and training all associates.

HealthLink complies with the HIPAA Security regulation through its WellPoint Information Security Program to:

- Maintain an information risk management program
- Protect the confidentiality, integrity and availability of electronic PHI
- Use administrative, physical and technical safeguards to address reasonably anticipated threats and hazards to electronic PHI
- Continually evaluate the effectiveness and adequacy of the program

HealthLink is committed to delivering excellent service. Part of that commitment includes complying with and supporting the HIPAA Security rule. Most importantly, we are committed to protecting member and patient privacy, and safeguarding related health information.

American Recovery and Reinvestment Act 2009 Readiness Disclosure Statement

We are committed to ensuring that our business processes, policies and procedures, processing systems and tools successfully meet the implementation requirements and deadlines mandated by the American Recovery and Reinvestment Act of 2009 (ARRA).

ARRA Overview

ARRA, also referred to as the Stimulus Act, is federal legislation that was signed into law by President Obama on February 17, 2009. Federal spending was extensive in implementing this legislation, involving substantial allocation for health information technology (HIT), including electronic health records, to help reduce the cost of health care.

Congress believed that it was important to enhance individual privacy rights within HIPAA to help offset the perceived risk associated with electronic medical records and other HIT programs. As the result, ARRA significantly changed health information privacy practices.

ARRA included a COBRA premium subsidy program, new Health Insurance Portability and Accountability Act privacy provisions and security requirements, and disclosure requirements for entities using electronic health records. Enhanced enforcement provisions have also been enacted, including increased monetary penalties for noncompliance.

ARRA requirements apply to covered entities including health plans, health care clearinghouses and health care providers who engage in electronic transactions under HIPAA and who receive, maintain or disclose individually identifiable health information. Under ARRA, HIPAA's privacy and security obligations now apply to business associates and must be incorporated into business associate agreements. All covered entities, and business associates who use or disclose protected health information (PHI) on a covered entity's behalf, were required to comply with the applicable standards by the specified compliance dates.

Privacy Provisions: Our Implementation Approach
Compliance Required and Achieved February 2009

A multifunctional project team was responsible for coordinating, communicating and implementing ARRA privacy provisions. The team included representation from the Project Management Office, Privacy Office, Legal, Information Technology and other business leaders within our company.

Four additional sub-teams were directly responsible for implementing, communicating and training related to these important privacy provisions, including:

- Breach Notification
- Business Associate Agreements
- Minimum Necessary, and
- Marketing.

General awareness messages and focused communications relaying ARRA's impact and relevant implementation details to all business areas were distributed throughout the company. New applications were designed and implemented to support expanded notification requirements and tracking accountabilities specified by privacy provisions within ARRA. Detailed processes were finalized and executed for each required provision.

Privacy Provision: Security Breach Notification
Compliance Required: September 2009

ARRA included an amendment to HIPAA called the HITECH Act. HITECH created a notification requirement for any breach, which is defined as the disclosure of PHI to an unauthorized party where that disclosure created a significant risk of reputation, financial or other harm. Individuals whose PHI is breached must be notified within 60 days of the covered entity's discovery of the breach. Breaches must also be reported to the secretary of Health and Human Services (HHS) and, in some instances, the local news media.

Breaches generally involve disclosure of PHI to an unintended recipient and include disclosures of “sensitive” personal information including, Social Security number, date of birth, diagnosis or treatment information, address, credit card or banking information.

Based on HITECH:

- The notification must be made within 60 days of the actual discovery of a breach or within 60 days of when the breach should have been discovered. The breach notification provision specifically requires that the notification be made by first-class mail or by substitute notice in certain circumstances
- If a breach impacts 500 or more individuals, the secretary of HHS must be notified. If 500 or more residents of a particular state or jurisdiction are involved in the breach, notice must also be made to a prominent media outlet. The secretary of HHS is obligated by this law to post a list of such breaches on the HHS website.
- All breaches are required to be logged and reported annually to the secretary of HHS

Privacy Provision: Business Associate Agreements
Compliance Required: February 2010

ARRA provides that certain privacy and security provisions found in HIPAA will apply directly to business associates. Under current HIPAA standards, only covered entities are regulated, and covered entities are responsible for passing along privacy obligations to their vendors and business associates. ARRA applies HIPAA privacy and security requirements directly to business associates and, therefore, allows for federal and state enforcement of HIPAA against business associates. In addition, ARRA requires business associate agreements to be amended to reflect the new ARRA requirements for business associates.

Privacy Provision: Minimum Necessary
Compliance Required: February 2010

ARRA requires covered entities to limit their distribution, use or requests for PHI, to the extent practicable, to a limited data set, or if more information is needed, to the minimum necessary amount of information needed to accomplish the intended purpose of the data use.

The Department of Health and Human Services is required to issue guidance on what constitutes “minimum necessary” within 18 months of the enactment of the Stimulus Act, after which such guidance will prevail.

ARRA provides several exceptions to the prohibition above:

- Public health activities
- Research, when the price charged reflects costs of preparing and transmitting data for such purpose
- Treatment, subject to regulations to be communicated
- Exchanges related to the sale or merger of a covered entity
- Remuneration by a covered entity to a business associate for activities involving the contracted exchange of data
- To provide an individual a copy of his or her PHI
- Any other reason determined as appropriate by the secretary of HHS.

The secretary of HHS is required to publish regulations to carry out this provision within 18 months of the effective date of the Stimulus Act (02/17/09), and the limitations expressed in this section will apply six months after the regulations are made known. This new rule will be effective after regulations relating to the sale of PHI are published.

HIPAA Privacy Final Rule 2013 Readiness Disclosure Statement

We committed to ensuring that our business processes, policies and procedures, processing systems and tools successfully meet the implementation requirements and deadlines mandated by the HIPAA Final Rule of 2013 (Final Rule).

HIPAA Privacy Final Rule Overview

The Final Rule, also known as the Omnibus Rule, was released on January 25, 2013, and makes important changes to the HIPAA Privacy Rule. We have established an enterprise project team to implement these requirements by the required compliance date of September 23, 2013.

Breach Notification

The Final Rule removes the “Risk of Harm” standard that was established in 2009 and replaces it with a new risk assessment requirement requiring a four-step analysis to determine whether the disclosure of PHI to an unauthorized third party created a low probability of compromise that the information would be misused. Covered entities must establish and document that the disclosure created a low probability of compromise by using the following criteria:

- The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

If a covered entity is not able to demonstrate a low probability of compromise, the disclosure constitutes a breach and HITECH notice must be sent the impacted individual.

Business Associate Agreements

The definition of a business associate has been expanded to include patient safety organizations, health information organizations, e-prescribing gateways, vendors of personal health records that provide services on behalf of a covered entity, and subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate. The expansion of the business associate definition is important because those individuals or entities falling within the definition are now subject to HIPAA’s Privacy and Security provisions.

The Final Rule expands the required elements of business associate agreements to include provisions requiring business associates to:

- Comply with the Security Rule with regard to electronic PHI
- Report breaches of unsecured PHI to covered entities
- Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate

Notice of Privacy Practices (NOPP)

Covered entities must make a number of material changes to their NOPPs and include several specific statements advising the individual of the following:

- The prohibition on the sale of PHI without the express written authorization of the individual;
- The duty of a covered entity to notify affected individuals of a breach of unsecured PHI;
- If the covered entity engages in fundraising, the requirement that the covered entity obtain a valid HIPAA authorization from the individual before using the individual's PHI for a fundraising purpose; and
- The right of the individual to restrict disclosures of PHI to a health plan with respect to health care for which the individual has paid out of pocket and in full.

Miscellaneous Provisions

Sale of PHI: The Final Rule prohibits the sale of PHI, except in certain limited circumstances, unless a valid HIPAA authorization has been obtained from the individual.

Genetic Information Non-Discrimination Act (GINA): The Final Rule modifies the Privacy Rule to incorporate certain requirements of GINA, requires that genetic information be treated as PHI and requires that language be included in NOPPs stating that covered entities cannot use genetic information for underwriting.

Information about Decedents: Requires safeguarding of PHI about a decedent for no more than 50 years after that individual's death and allows certain information to be shared with appropriate individuals.

Marketing: If the covered entity receives remuneration for marketing, a valid HIPAA authorization must be obtained before use.