"People helping people help themselves"

Mitchell E. Daniels, Jr., Governor
State of Indiana

Indiana Family and Social Services Administration
402 W. WASHINGTON STREET, P.O. BOX 7083
INDIANAPOLIS, IN 46207-7083

To: ALL DDRS Staff

From: DDRS Communications

Re: Changes to HIPAA Regulations

Date: March 19, 2010

With the American Recovery and Reinvestment Act (ARRA) signed into law by President Obama on February 17, 2009, come many changes to privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Covered entities and their business associates should become familiar with these changes and take any necessary steps to comply with the new requirements.

One of the many changes to HIPAA included in the ARRA requires all covered entities to modify their contracts with business associates who process Protected Health Information (PHI). Therefore, FSSA is in the process of revising all active contracts to reflect the new HIPAA laws. The Division of Disability and Rehabilitative Services (DDRS) recognizes that we all must be proactive in protecting the personal information of the individuals we serve. In general, our process for sharing information has not changed under the new rules. What has changed is that the liability is now significantly higher for inappropriate disclosures. Please take caution and remember to follow the HIPAA guidelines when sharing information about consumers.

We ask you to review the following pages carefully. If you have any questions or feedback regarding the impact of this information on your daily work activities, you should contact your supervisor. In the meantime, we are preparing updates to the HIPAA training, which will be available to you in the coming weeks.

The FSSA HIPAA Compliance Office is conducting a risk assessment to determine how the changes might impact FSSA business units. Please contact H. Cliff McCullough, Director of the FSSA Project Management HIPAA Compliance Office, at cliff.mccullough@fssa.in.gov, (317) 232-4732 if you have questions about this assessment.

Thank you.

Current Projects Security/Privacy Assessments 501Conversion Planning

Background:
The American Recovery and Reinvestment Act (ARRA) of 200included needed improvements to the HIPAA Privacy and Security Standards under the Health Information Technology for Economic and Clinical Health (HITECH) component of the Act. ARRA became law February 17, 2009; compliance with most of the changes must be in place by February 17, 2010.

HITECH not only improved certain privacy and security protections (including new requirements for breach notifications if a person's health information is improperly used or disclosed), but also added enforcement muscle to HIPAA. In particular, the civil fines for non-compliance were significantly increased (and can now be shared with injured parties), state attorneys general can bring enforcement action against covered entities that violate the rules, and HHS is required to conduct periodic audits to ensure covered entities are in compliance with the privacy and security rules. For state agencies like FSSA, failure to comply may also have federal funding impacts.

Last year CMS published revised rules regarding the standards to be followed for electronic transactions, such as claims and payments, between payers (e.g., insurance companies, Medicare, Medicaid) and providers (hospitals, physicians, clinics, etc.)This necessitates a conversion from the current standards to the new standards, which is to be completed by December 31, 2011.

Privacy Standard (Federal Law Regulations)

Establishes privacy protections over a person's medical and certain other information, and provides remedies (e.g., civil and criminal penalties) for violations of those protections.

The term PHI (Protected Health Information) is commonly used to describe health information about a person (e.g., illness, physical status, medications, etc.) that can be associated with that person (e.g., name, address, social security number, medical record number, etc.).

The Privacy Standard (or Rule) predominately requires the Covered Entity (CE) to develop, implement, and maintain written policies and procedures (appropriate for their organization) to protect the privacy and security of a person's PHI. These privacy policies and procedures must reflect the requirements of the Privacy Standard.

The Privacy Standard requires that the CE take reasonable steps to protect the privacy and security of PHI (in its safekeeping) in all forms electronic, paper, and verbal.

Covered Entities (CE)those organizations that must comply with this law and regulations include all health plans (pays for medical care), including Medicare and Medicaid, most provider organizations (hospitals, physicians, labs, clinics, pharmacies that provide medical care and services), and healthcare clearinghouses.

CEs must be in compliance with HIPAA Privacy as of April 14, 2003.

Security Standard (Law Regulations)

Establishes high-level standards over the security of PHI in electronic form (sometimes referred to as E-PHI), including technical, physical, and administrative controls and procedures.

The Security Standard is designed to support and fulfill the requirements of the Privacy Standard to protect the privacy and security of PHI in electronic form. Thus, compliance with the Security Standard is required to be in compliance with the Privacy Standard.

The Security Standard requires the CE to develop, implement, and maintain written policies and procedures (appropriate for the organization) to protect the privacy and security of a person's E-PHI.

Generally stated, the Security Standard is not prescriptive with respect to the types of standards or technologies a CE should follow to secure PHI, but rather establishes at a high level the types of security controls that should be in place.

For example, the Standard requires that access controls be in place over access to E-PHI and that users must be uniquely identified; it does not specify what type of access controls are to be used (e.g., passwords, biometrics, tokens, etc.), nor does it specify how users are to be uniquely identified (e.g., user ID, biometrics), nor whether single factor or dual factor authentication is needed. The determination of these types of specifics is up to the CE based on what's appropriate given the CEs size, complexity, and sophistication.

That said, in certain instances specific industry standards are referenced. For example, NIST Special Publications 800-52 and 800-77 are referenced as acceptable standards for the encryption of E-PHI during transport.

The Covered Entities that must comply with the Security Standard are the same as those that must comply with the Privacy Standard. CEs must be in compliance with the Security Standard as of April 20, 2005.

Transactions Code Sets (TCS) Standard (Law Regulations)/501Conversion

Establishes that certain, common electronic business transactions between payers (insurance companies, government) and providers follow particular ANSI X12N 401transaction standards to reduce the ambiguity and cost of performing those transactions establishes uniform content and structure to promote data uniformity, quality, and usability; and, to lower processing costs.

These common electronic business transactions include claims (professional, institutional, dental), eligibility verification, referral/authorizations, claim status verification, enrollment, claim payment/remittance, premium payments, COB, and retail pharmacy (claims, eligibility, payment, COB).Note retail pharmacy transactions will follow the NCPCP standards for drugs and biologics; the X12N standards for all other claims (e.g., DME).

The TCS standard also mandated the use of particular medical coding sets, such as ICD-9.

Initially, CEs (health plans, healthcare clearing houses, and providers who conducted these transactions electronically) were to comply with the TCS Standard by October 16, 2002; however, extensions were granted by HHS/CMS due to industry readiness (or lack thereof).By 2004 most CEs were in compliance.

In January, 200HHS/CMS published revised TCS rules mandating conversion from the 401transaction standards to the new 501standards.The purpose in doing so was to further improve the standardized content of these transactions (based on learning gained during the preceding years use of the 401standard), to improve the quality of the medical data collected, and in preparation for the industry's conversion to the ICD-1medical coding standard. Updated NCPDP standards are also mandated.

By December 31, 201CEs must be able to demonstrate that they can send, receive, and process the 501standards through internal testing.

By December 31, 2011 CEs must have completed end-to-end testing (between payers and providers).

By January 1, 2012 CEs must be using the 501standard.

To meet the 501standard, system upgrades will be required and business processes may be impacted with respect to capturing the new or revised data elements.

FSSA Security/Privacy Assessment 501Conversion Planning
HIPAA Privacy/Security/TCS Summary

Reference #: DDRS Staff 20100319