To: County Officials

From: Alissa Smith, Dorsey & Whitney LLP

Date: 11.27.2013

Re: New HIPAA Manual

I. Introduction

In 2009, as part of the American Recovery and Reinvestment Act (the "ARRA"), a number of significant changes were made to the Health Insurance Portability and Accountability Act ("HIPAA") and additional changes were required to be made by future regulation. On January 17, 2013, the Department of Health and Human Services issued the HIPAA Final Rule that included a large number of changes to HIPAA. As part of the Iowa State Association of Counties' HIPAA compliance efforts, we have adopted a revised and updated HIPAA Manual to incorporate these numerous changes to HIPAA which govern our operations through ETC and the health plan related to individually identifiable health information. We have also had a similar updated and comprehensive HIPAA manual created for adoption by our members who have health care provider and health plan operations that involve the use or disclosure of individually identifiable health information. The revised and updated HIPAA Manual for ISAC and our members also includes updated policies that address state laws which provide greater protection for health information, such as Iowa's Mental Health Privacy Law, and includes sample forms and contracts to use for achieving HIPAA compliance.

A copy of the new HIPAA Manual is enclosed, and a summary of the main changes in the HIPAA Final Rule is included below.

II. Summary of the Main Changes to HIPAA under the Final Rule

The major changes to HIPAA under the HIPAA Final Rule are outlined below.

A. Breach Notification

The ARRA added a new breach notification rule to HIPAA which requires covered entities to report certain breaches to the affected individuals, to the government, and, in some cases, to media outlets. Following the ARRA in 2009, an interim breach notification rule has been in place for several years. The HIPAA Final Rule made several significant changes to the interim breach notification rule. For example, the required analysis of a breach has changed to require a covered entity to presume that a breach has occurred in the event of "the access, acquisition, use or disclosure of unsecured PHI not permitted under the Privacy Rule that compromises the security or privacy of the PHI" unless the covered entity can demonstrate through a risk assessment that there is a low probability the PHI has been compromised. This change in the required analysis of a breach will likely result in a significant increase in the number of "breach" incidents that must be reported to individuals and to the government. You can find more information about the breach notification rule by reviewing the Breach Notification Policy (and the accompanying flowchart and risk assessment tool) in the HIPAA Privacy Manual.

B. Business Associates

The ARRA included significant changes to HIPAA for individuals and entities that are "business associates" of covered entities. One of the main changes was that the HIPAA Security Rule now directly regulates business associates. Additionally, the HIPAA Final Rule added several provisions of the HIPAA Privacy Rule that directly regulate business associates. The HIPAA Final Rule also modified the definition of "business associate" to include additional individuals/entities such as subcontractors, subcontractors of subcontractors, entities that maintain PHI (including hard copies and electronic data such as maintained by cloud providers), entities that provide data transmission services, health information organizations, e-prescribing gateways, and persons that offer a personal health record to one or more individuals on behalf of a covered entity. Additionally, the HIPAA Final Rule changed the terms which are required to be included in business associate agreements. You can find more information about these changes in the Business Associate Assurances Policy in the HIPAA Privacy Manual. The HIPAA Privacy Manual also includes a template Business Associate Agreement.

C. Marketing and Sale of Protected Health Information ("PHI")

The HIPAA Final Rule requires covered entities to obtain an individual's authorization before almost any communication to the individual that is considered "marketing". More information about the new marketing rule can be found in the Marketing Policy in the HIPAA Privacy Manual.

Under the HIPAA Final Rule, covered entities cannot disclose PHI in exchange for remuneration unless they receive an authorization that explicitly states the covered entity will receive remuneration for disclosing the individual's PHI. You can find more information about this change in the Sale of PHI Policy in the HIPAA Privacy Manual.

D. Right to Access

Under the HIPAA Final Rule, generally, if an individual requests an electronic copy of PHI maintained electronically, the covered entity must provide that individual with access in the electronic form and format requested by the individual if readily available. A covered entity has thirty days to act on a request, plus one thirty day extension if needed, and may impose a reasonable, cost-based fee for access. You can find more information about the HIPAA rules on accessing PHI in the Accessing PHI Policy of the HIPAA Privacy Manual.

E. Restriction on Disclosures

The HIPAA Final Rule requires covered entities to agree to an individual's requested restriction on disclosure to a health plan if the disclosure (i) would be for payment or health care operations, (ii) is not otherwise required by law, and (iii) pertains solely to health care items or services the individual paid for out of pocket in full. You can find more information about these restrictions in the Requests for Privacy Protection for PHI Policy in the HIPAA Privacy Manual.

F. Notice of Privacy Practices

The HIPAA Final Rule made a number of changes to the requirements for the Notice of Privacy Practices. First, the Notice of Privacy Practices must include a number of additional statements regarding (i) authorization for marketing, psychotherapy notes, and sale of PHI; (ii) individual right to restrictions; and (iii) breach notification. Second, covered entities that are health care providers must provide a revised Notice to first-time patients and make the revised Notice available at service delivery sites for patients, post the Notice in physical locations of

service delivery, and post the Notice electronically on a website that describes services. There are different notice obligations for health plans. Health care clearinghouses do not have obligations under this rule (unless they maintain a website that describes services provided). You can find more information about the rules on notices of privacy practice in the Notice of Privacy Practices Policy in the HIPAA Privacy Manual.