NELSON HARDIMAN
HEALTHCARE LAWYERS

Takeaways From the Newly Published HIPAA Omnibus Rule

On January 25, 2013, the Department of Health and Human Services published the long anticipated Omnibus Rule which amends the Health Insurance Portability and Accountability Act (HIPAA) and the privacy and security provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. As Leon Rodriguez, the Dire of the Office for Civil Rights, the office that enforces HIPAA, has indicated, “This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented.” Here are six practical takeaways of the Omnibus Rule that healthcare providers should be aware of:

1) More security incidences are reportable

The new Rule has made significant changes to the data breach notification requirements that will make it more likely that a br report will have to be made. Under prior law, a breach only had to be reported if it posed a “significant risk of financial, reputat or other harm to the patient.” The new Rule creates a new presumption that the unauthorized acquisition, access, use, or disclosure of protected health information is a data breach unless a Covered Entity or business associate demonstrates that t is a low probability that the protected health information (PHI) was compromised. This new requirement will make it more diffi justify the failure to make a breach report. Under the new Rule, in the event of an incident that could be a potential data breac covered entities and business associates must conduct and document a risk assessment and determine whether there is a lo probability that PHI has been compromised by performing a risk assessment. Unless the provider or business associate cond the risk assessment and makes this finding, a disclosure must be made.

To comply with the Rule, we recommend that health care providers perform a gap analysis to determine what policies and procedures need to be changed, review and revise their risk assessment procedures, and breach notification and response pl to ensure that they comply with the Rule and other HIPAA requirements; review the methods for conducting risk assessments determine when and under what circumstances breach notification is required, and whether if a breach is discovered, the organization could respond within the required time periods. As always, workforce members must be trained properly to comp with HIPAA and with the changes made by the new Rules.

2) Increased liability for Business Associates, Subcontractors of Business Associates are now Business Associates

Business associates are now directly liable for violations of the HIPAA security, privacy, and data breach rules, and are subje civil and criminal penalties for failure to comply with the applicable provisions. For the first time, business associates will be required to obtain written business associate agreements (BAAs) from their subcontractors and to take reasonable steps to cu the breach or terminate the contract in the event of a material breach by the subcontractor.

The new Rule modifies the definition of business associates to include subcontractors, which means that business associate liability now covers to all subcontractors involved in the chain of data flow. Several new entities, including those that provide d transmission of PHI, such as health information exchanges, e-prescribing gateways, and cloud service providers, as well as d storage companies and other entities that create, receive, or transmit PHI on behalf of business associates are now business associates themselves, and are subject to direct liability under HIPAA Privacy and Security Rules.<

To comply with the Rule, we recommend that health care providers ensure that they have a Business Associate Agreement w subcontractors, ensure that subcontractors comply with HIPAA, and ensure that the Agreement complies with the new Rule. T may be a surprise for subcontractors who are not in the health care field and others who do not consider themselves business

associates, and would rather not take the responsibility of being a business associate. However, because the Rule shifts the responsibility from the Covered Entity to the Business Associate with regard to its subcontractors' compliance with the Rule, subcontractors will have new legal obligations under the HIPAA Privacy and Security Rules and must take action in order to b themselves in compliance with the new Omnibus Rule.

3) Enforcement moves toward an increasingly punitive system

The new Rule requires the Department of Health and Human Services to implement a mandatory, tiered penalty system and t move away from the voluntary compliance framework used in the past. Penalties now range from $100 to $50,000 per violatio depending on the level of knowledge and willfulness of the entity, with a $1.5 million cap per calendar year for multiple violatio identical provisions. The new Rule also provides that civil and criminal penalties can now be applied directly to business associates. The Department of Health and Human Services will also have the ability to share information with other law enforcement agencies such as the Attorney General or the Federal Trade Commission.

4) Enhanced patient rights to E-records and restrictions on disclosure

Patients now have a right to obtain a copy of their health records in electronic form when such information is maintained by a Covered Entity in electronic form in a designated record set. Covered Entities must provide the electronic copy in a format mu agreed upon by the patient and the Covered Entity. Notably, the Rule provides that if requested by the patient, the Covered E may provide the electronic copy of PHI through unencrypted e-mail, provided that the Covered Entity advises the patient of th of doing so. In such a case, the Covered Entity would not be responsible for any unauthorized access of PHI during transmiss for safeguarding PHI once the PHI is delivered to the patient. Patients also have enhanced rights under the Rule to restrict disclosure of PHI to health plans for treatments and services paid for in cash.

In addition, the new Rule provides patients with the right to direct Covered Entities and Business Associates to transmit an electronic copy of the record directly to a person or entity designated by the patient, regardless of whether the PHI is in electro or paper form. The Rule also shortens the time frame available to Covered Entities for providing access to records. Under the Rule, Covered Entities must provide access to all paper and electronic PHI within 30 days of the patient's request with the opt a one-time 30-day extension.

To comply with the new Rule, we recommend that health care providers review and understand the new rights that patients ha ask for and restrict disclosure of their PHI, consider the use of encryption for PHI, and train workforce members to comply with Rule.

5) Notices of Privacy Practices must be revised

The Rule also requires changes in the Notice of Privacy Practices. The HIPAA Notice of Privacy Practices must now include a statement regarding the right of affected patients to be notified following a data breach and the Notice must also describe cert uses and disclosures of PHI that require patient authorization. The Department of Health and Human Services considers thes modifications to the privacy Notice to be material requiring Covered Entities to provide new Privacy Notices to patients. Althou the Privacy Rule generally provides health plans 60 days following a material revision to mail revised Notices to members, the Department of Health and Human Services is providing a reprieve by permitting health plans that post their Notice on their we to post the revised Notice on that website by the new Rule's compliance date (September 23, 2013).

To comply with the new Rule, we recommend that Covered Entities amend their Notice of Privacy Practices, review and revis privacy and security policies and procedures to comply with the Rule, and train workforce members to comply with the new R

6) Strengthens protection of genetic information under the Genetic Information Non-Discrimination Act (GINA)

The new Rule strengthens the privacy protections for genetic information by including genetic information as a type of PHI sul to HIPAA. The Rule also adds definitions to the Genetic Information Non-discrimination Act (GINA), including definitions for fa member, genetic information, genetic services, and genetic test which provide that family health history is now considered "ge information" covered by the Act. The Act also prohibits health plans from using or disclosing genetic information for underwriti purposes.

Conclusion

In light of the new requirements under the Omnibus Rule, all members of the health care industry should review their Privacy

Security policies and procedures to ensure that they comply with the new requirements. Our office is available to assist you in effort. Nelson Hardiman LLP regularly advises clients on issues related to HIPAA and the HITECH Act and can help bring you company into compliance with the new Omnibus Rule.

About the author:

Farooq Mir, Esq. is an associate with the firm and advises health care providers on aspects of health care law. Nelson Hardim a Los Angeles law firm that specializes in health care law and compliance. For further information or assistance, contact Fmir@nelsonhardiman.com.