HIPPA Update

It has been more than a decade since most providers first undertook HIPAA privacy compliance efforts. Since these initial compliance efforts, many new rules and regulations have been enacted and impact the manner in which health care providers must operate. However, many providers have not been diligent in continuing their compliance efforts. HIPAA compliance is an ongoing process. It is not enough to adopt written policies and procedures. These policies and procedures must be periodically reviewed and updated. New hires should be trained on the policies and procedures. Staff training should be undertaken regularly. Providers must create a culture of concern for patient privacy and health information security.

During 2012, the Office of Civil Rights (OCR) of the Department of the Health and Human Services (HHS) conducted audits of covered entities during Phase 1 of its audit program. Under HIPAA, OCR is required to conduct periodic audits. Phase II, which was to commence in October 2014, has been delayed. OCR also stated that Phase II will involve more on-site comprehensive audits and fewer desk audits than planned.

The present delay in the start of the Phase II compliance audits is an opportune time to conduct a HIPAA self-assessment and tighten up any gaps in compliance.

HIPAA compliance is not optional. There have been many recent reported instances of HIPAA violations. Fines and penalties can be substantial, in addition to the time and resources that providers must devote to responding to any breach or complaint lodged with OCR .

Summary of Recent HIPPA Changes

Among the recent changes to the HIPAA Privacy and Security rules are:

- A revised Notice of Privacy Practices (NPP) *must be distributed to all patients*.
- The revised NPP must be redistributed, including posting on your website.
- Privacy and security requirements are extended to Business Associates and their contractors and require updates to Business Associate Agreements.
- New limitations on the use of protected health information for marketing and fund-raising purposes.
- Sale of a patient's personal health information without individual authorization is prohibited.
- Expanded patients' rights to request and receive electronic copies of their personal health information.

Notice of Privacy Practices

The NPP must be updated to include these additional elements:

- A statement that certain uses and disclosures of protected health information (PHI) require an authorization from the subject individual, specifically psychotherapy notes (if recorded or maintained by the Covered Entity), PHI for marketing purposes and in instances constituting the sale of PHI;
- A statement that uses and disclosures not addressed within the NPP require a written authorization;
- An acknowledgment that the individual may revoke any authorization granted for uses and disclosures requiring such authorization; and
- A notice of the individual's rights following a breach of unsecured PHI, which can be sufficiently accomplished with a statement that the individual has a right to or will receive notification of a breach of the individual's unsecured PHI.

What to Do Now

- Notify individuals of these new rights through the revised NPP.
- NPPs must be available and posted at the

provider's location where services are provided. Make copies of the entire policy available to existing patients at their request.

- Post the revised NPP on your website.
- Each new patient should given a complete copy of the revised NPP and must return a good faith acknowledgment of receipt.

Business Associates

Under the recent amendments to HIPAA, Business Associates are directly regulated and responsible for complying with HIPAA. As of September 23, 2014, all Business Associate Agreements must reflect the new requirements.

The new rule expands the definition of "Business Associates", by including: subcontractors who create, receive, maintain or transmit protected health information on behalf of a Business Associate; health information organizations, e-prescribing gateways, and certain other persons that provide data transmission services for covered entities; and persons that offer personal health records on behalf of a covered entity.

These new requirements include the following:

- Require that the Business Associate comply, and require its subcontractors to comply, with applicable requirements of the HIPAA Security Rule;
- Require that the Business Associate ensure that its subcontractors agree to the same restrictions and conditions that apply to the Business Associate with respect to PHI;
- Require that the Business Associate report breaches of unsecured PHI to the covered entity;
- If the Business Associate carries out a covered entity's obligation under the Privacy Rule, require that the Business Associate comply with the Privacy Rule requirements that apply to the performance of such obligation; and
- Require the Business Associate take steps to cure or end the violation (or terminate the relationship) if it knows of a pattern of activity or practice of its subcontractor that constitutes a material breach of the subcontractor's obligations.

What to Do Now

- Identify all Business Associates.
- Review existing Business Associate Agreements and amend to comply with the new rules. Ensure that all Business Associates execute an updated Business Associate Agreement.
- Continue to exercise diligence in establishing and monitoring Business Associate relationships.

Conclusion

This is a perfect time to review your HIPAA compliance program. It is not too late to become compliant. In addition to the action items identified above, we recommend the following:

- Ensure that your organization's Privacy Officer and Security Officer are up to date on the new rules.
- Conduct a risk assessment to determine the likelihood of a data breach.
- Review and update HIPAA Privacy and Security policies, including those related to Business Associates and Notice of Privacy Practices.
- Retrain the workforce on updated policies and procedures and establish a schedule for on-going training.
- Establish monitoring and internal audits to avoid lapses in the privacy and security of PHI.

If you have questions or need further information about HIPAA compliance, contact Paul Gilman at (312) 755-3168 or the Aronberg Goldgehn attorney with whom you work.