Wolters Kluwer
Health Law Daily
July 20, 2016
Wolters Kluwer

INDUSTRY NEWS

COMPLIANCE NEWS—Privacy policies, due diligence and the use of confidentiality agreements with vendors

By Harold Bishop, J.D.

Health care plans and providers must take steps to maintain control of and protect against the misuse of employee data, trade secrets, and patient data, both by their business associates (BAs) and other non-BA vendors. In a recent Health Care Compliance Association (HCCA) webinar, William J. Roberts of Shipman & Goodwin discussed a strategy to accomplish this goal through the use of organizational policies, due diligence in selecting vendors, and confidentiality agreements with vendors.

Organizational policies. With regards to the development of organizational policies, Roberts cautioned that plans and providers should not limit their privacy and security policies to HIPAA, but should also address proprietary information, trade secrets, and state privacy laws. He also recommended that their policies apply to all vendors (e.g., cleaning services and others with access to the premises and information systems), not just BAs. Roberts suggested that plans and providers revisit their old policies regarding access to premises and information systems and determine when they should ask a non-BA vendor to enter into a confidentiality agreement.

Due diligence. In selecting vendors, Roberts suggested using a vendor screening tool to obtain privacy and security assurances from a potential vendor prior to negotiating a contract. This would give plans and providers assurance that the vendor is aware of privacy and security requirements and has their own plan in place. Roberts also recommended using the screening tool to periodically monitor and remind the vendor of privacy and security expectations.

Confidentiality agreements. Roberts discussed four options for binding vendors to confidentiality requirements: (1) the business associate agreement (BAA); (2) the traditional non-disclosure agreement; (3) putting confidentiality language into a standard vendor service agreement; and (4) attaching a compliance addendum to the standard service agreement.

Vicarious liability. Roberts strongly recommended structuring vendor agreements to avoid vicarious liability. Under the theory of vicarious liability, a health plan or provider may be liable for the acts or omissions of its BAs, and a BA may be liable for the acts or omissions of its subcontractors. The key factor, according to Roberts, is whether the plan or provider has control over the conduct of the BA or subcontractor. If so, the BA or subcontractor is likely an agent and the plan or provider will likely be subject to vicarious liability.

In drafting the vendor agreement, Roberts believes that language saying "not an agent" is not enough to avoid vicarious liability. Instead, agreements should be narrowly tailored to specific tasks and obligations of the vendor. This, according to Roberts, will reduce the amount of control the plan or provider has over the conduct of the BA or subcontractor.

BAAs. In drafting and negotiating BBAs, Roberts recommended focusing on the following key terms and provisions:

- **Breach notification.** Require the BA to notify the plan or provider of a breach of unsecured (i.e., unencrypted) protected health information (PHI) as soon as practicable but no more than the 60 days required by HIPAA.
- **Breach mitigation.** Require the BA to take reasonable steps (include specific actions) to mitigate any potential harm from the breach.
- **Cooperation.** Include a provision requiring the BA to participate in the investigation and provide the information the plan or provider needs.
- **Indemnification.** Include a provision stating that the BA is responsible for all costs incurred by the plan or provider due to a breach or violation of the law or the BAA. The provision should specify the costs for which the BA will be responsible (e.g., attorney's fees, notification costs, etc.).
- **Insurance.** Because an indemnification clause is only as good as the BA's ability to pay, require cyber liability insurance (standard liability and malpractice policies will not cover PHI breaches).
- **De-identification of PHI.** Because many vendors seek the right to de-identify PHI to use for their own purposes, such as quality control and research, require that any de-identification be performed in accordance with HIPAA, that plan and provider identifiers be removed, and hold the BA responsible for improper de-identification.
- **Security safeguards.** The agreement should: (1) mandate that the vendor encrypt PHI when it is stored or emailed; (2) mandate that the BA enter into confidentiality agreements with it employees with PHI access; (3) require adherence to applicable state laws and standards; and (4) prohibit storage of PHI on personal devices or servers.
- **Change of law.** Because HIPAA and its implementing regulations are constantly being amended, the BAA should state that the plan or provider has the right to amend the agreement in the event of a change in the law or regulations.

Non-BA vendor agreements. While BAAs are crucial, Roberts warned that plans and providers should not ignore the need for confidentiality clauses or agreements for non-BA vendors or other third parties. According to Roberts, the key terms and provisions in those agreements should include a commitment to confidentiality, compliance with laws and policies, breach incident reporting, and reimbursement.

Attorneys: William J. Roberts (Shipman & Goodwin).

Companies: Health Care Compliance Association

IndustryNews: NewsStory ComplianceNews ConfidentialityNews CorporateNews HITNews HIPAANews DisclosureNews