Vorys Benefits Brief: Responding to a Breach of HIPAA-Protected Information - Guidance for Employers

Related Professionals

Jennifer Bibart Dunsizer

Christine M. Poth

Elizabeth Howard

Jacquelyn Meng Abbott

Related Services

Employee Benefits and Executive Compensation

Employment Counseling

Labor and Employment

CLIENT ALERT | 4.15.2026

On January 13, 2025, Conduent Business Services LLC (Conduent) discovered it was the subject of a cybersecurity incident involving unauthorized access to its systems between October 21, 2024, and January 13, 2025. The incident may have affected more than 25 million individuals, including more than 15.4 million Texas residents. This incident is a reminder that health plans may have HIPAA and contractual obligations even when a breach occurs at a third party.

Background

Conduent provides back-office, payment, mailing, and other administrative support services to health care organizations, insurers, and government entities. Public reporting indicates that the incident may have begun with compromised VPN credentials. Reports also suggest that the threat actor moved laterally within Conduent's data environment, exfiltrated data, and deployed ransomware.

The data involved appears to vary by individual, but it may include names, dates of birth, addresses, Social Security numbers, health insurance information, treatment and diagnosis codes, provider names, dates of service, claim amounts, group numbers, and subscriber numbers. The incident has drawn significant regulatory and legal attention, including an investigation by the Texas Attorney General and multiple reported lawsuits.

For HIPAA purposes, a covered entity includes a health plan, a health care clearinghouse, or a health care provider that transmits health information electronically in connection with a covered transaction. An employer is not automatically a covered entity simply because it sponsors a group health plan, but the group health plan itself may be a covered entity. An entity becomes a business associate if, on behalf of a covered entity, it creates, receives, maintains, or transmits protected health information (PHI) for a HIPAA-regulated function or activity, such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, or repricing. An entity also may be a business associate if it provides

certain services to or for a covered entity involving PHI, such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. A subcontractor of a business associate can be a business associate under HIPAA. A covered entity may be a business associate of another covered entity.

The Conduent data breach may trigger HIPAA obligations for both affected health plans and their business associates. If a breach of unsecured PHI affects 500 or more individuals, the covered entity must notify Health and Human Services (HHS) without unreasonable delay and no later than 60 calendar days after discovery. If a breach affects fewer than 500 individuals, the covered entity must notify HHS within 60 days after the end of the calendar year in which the breach was discovered, although earlier reporting is permitted. The covered entity generally must notify affected individuals without unreasonable delay and no later than 60 calendar days after discovery. A business associate may submit the breach report on behalf of all the plans it services and the insurer of insured health plans routinely files for all the health plans it insures. The practice is more split for self-insured plans. The parties should confirm their respective responsibilities under the applicable business associate agreement and related contracts.

Key Takeaways for Employers

The Conduent incident is one of the largest reported health care data breaches in U.S. history and appears to have involved sensitive personal and protected health information. Even when a breach occurs at a third-party subcontractor, the employers' health plans may still have obligations under HIPAA. Because of the significant potential penalties for failure to report a breach, it is important to for employers with self-funded group health plans to take prompt steps to assess whether the plan's data has been affected and whether any obligations have been triggered for the plan. Here are recommended next steps:

1. **Determine whether your organization is affected:**
    - Ask your plan's TPA to confirm whether Conduent managed any plan data for your group health plan. If so, identify the categories of your plan data that may have been affected by this data breach.
2. **Confirm the legal role of the affected arrangement:**
    - Evaluate whether the data relates to the group health plan as a covered entity and whether Conduent or another vendor was acting as a business associate.
3. **Review business associate agreements and service contracts:**
    - Examine business associate agreements, administrative services agreements, and other vendor contracts for notice deadlines, cooperation requirements, indemnification provisions, and allocation of reporting responsibilities. This review will help the employer determine who bears the obligation and cost of reporting the breach.
4. **Assess notice and reporting obligations.:**
    - Determine whether notice to affected individuals, HHS, state regulators, or other parties is required, and whether a business associate will report on behalf of the covered entity.
5. **Coordinate an internal response team.**
    - Include legal, privacy, benefits, HR, IT, security, and communications personnel as appropriate so that the response is accurate, timely, and documented.

6. **Prepare communications for affected individuals and stakeholders.**
    - If notice is required, prepare clear communications explaining what happened, what information may have been involved, and what protective steps are available.
7. **Document response efforts.**
    - Keep records of what action was taken, when the incident was discovered, what notices were considered or sent, and what mitigation steps were taken.
8. **Review and strengthen safeguards**.
    - Reassess vendor oversight, access controls, incident response procedures, logging and risk analysis practices to reduce future exposure.
9. **Consult legal counsel.**
    - Collaborate with counsel to assess HIPAA compliance obligations, state law requirements, contractual rights, and potential liability.

Note that additional obligations apply if the employer is also an affected provider who uses Conduent, either directly or indirectly.

For questions or additional information about this Vorys Benefits Brief and its application, consult with legal counsel.