Provided by Kinloch Consulting Group, Inc.

LEGAL UPDATE

Kinloch CONSULTING GROUP
An Optisure Risk Partner

March 20, 2023

HIGHLIGHTS

- HHS provided two annual reports on HIPAA compliance covering the 2021 calendar year.
- These reports are intended to help covered entities and business associates (regulated entities) comply with the HIPAA Privacy, Security and Breach Notification Rules.
- The reports emphasize the need for regulated entities to continue working on improving HIPAA compliance, particularly with respect to security requirements for PHI.

HHS Provides Annual Reports on HIPAA Compliance and Breaches

The Department of Health and Human Services (HHS) recently shared two reports on compliance with HIPAA's privacy, security and breach notification requirements for 2021. According to HHS, these reports highlight where HIPAA-regulated entities (including health plans and business associates) should focus their HIPAA compliance efforts.

The reports identify steps taken by HHS' Office for Civil Rights (OCR) to investigate complaints, breach reports and compliance reviews regarding potential violations of the HIPAA Rules. The reports also include important data on the number of HIPAA cases investigated, areas of noncompliance, and insights into trends such as cybersecurity readiness.

HIPAA Compliance

The first report, HIPAA Privacy, Security and Breach Notification Compliance, identifies the number of HIPAA complaints received, the method by which those complaints were resolved, the number of compliance reviews initiated by OCR and the outcome of each review. The report highlights the following enforcement actions during the 2021 calendar year:

- OCR received 34,077 new complaints alleging HIPAA violations, a 25% increase from the number of complaints received in 2020. OCR also initiated 674 compliance reviews to investigate allegations of HIPAA violations that did not arise from complaints;
- OCR required hundreds of regulated entities to take corrective action and imposed significant civil penalties (or agreed to monetary settlements in lieu of penalties) for 17 regulated entities; and
- The top issues alleged in HIPAA complaints were impermissible uses and disclosures, right of access, safeguards, and breach notification to individuals.

HIPAA Breach Notification

The second report, Breaches of Unsecured Protected Health Information (PHI), identifies the number and nature of breaches of unsecured PHI that were reported to HHS in 2021 and the actions taken in response to those breaches. It also highlights the continued need for regulated entities to improve compliance with the HIPAA Security Rule requirements. Such compliance improvement measures include risk analysis and risk management, information system activity review, audit controls and access controls.

As in previous years, hacking/IT incidents remained the most prominent type of breach, affecting 500 or more individuals and comprising 75% of the reported breaches. The location with the most breaches affecting 500 or more individuals was network servers. For breaches affecting fewer than 500 individuals, the most prominent category of breaches was unauthorized access or disclosures, and the most prevalent location was paper records.