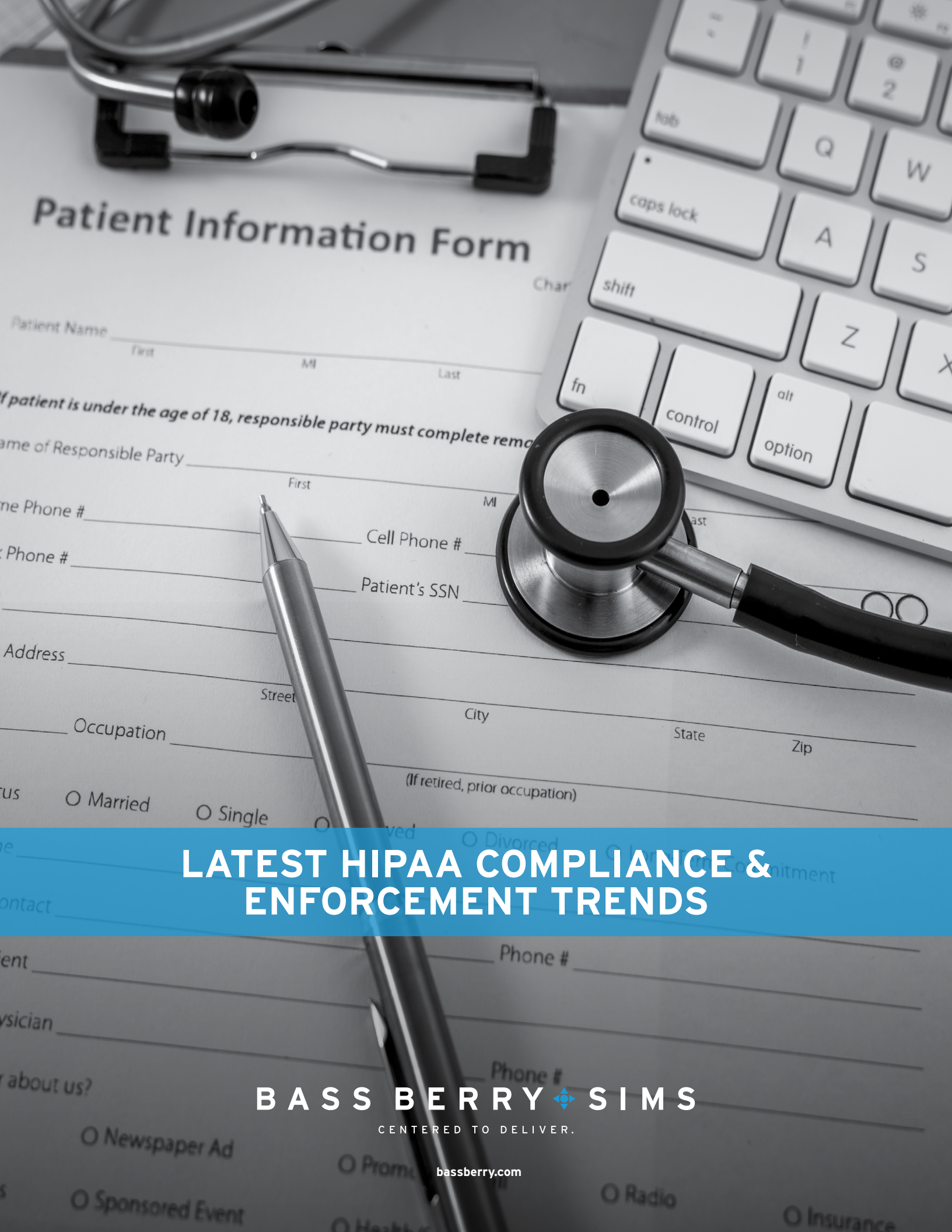


LATEST HIPAA COMPLIANCE & ENFORCEMENT TRENDS

BASS BERRY + SIMS

CENTERED TO DELIVER.

bassberry.com

Enforcement activity by the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) showed no signs of slowing throughout 2018 and has already picked up speed in 2019. More recent and significant actions from OCR last year include the following:

- OCR began 2019 with a recovery of a $3 million settlement and corrective action plan based on two reported breach incidents: one was an update to security settings that unintentionally permitted access to an otherwise unprotected server, which made protected health information (PHI) accessible to anyone with access to the server; and the second breach resulted from a misconfiguration during a response to an information technology (IT) troubleshooting ticket, which exposed unsecured PHI over the internet. OCR also found that the provider failed to perform periodic evaluations in response to operational changes and failed to obtain a written business associate agreement (BAA) with a PHI contractor. OCR said the resolution is a reminder that "information security is a dynamic process, and the risks to electronic PHI (ePHI) may arise before, during and after implementation" of system changes.
- In the Spring of 2019, HHS OCR moved to quarterly newsletters, providing ongoing "recommendations" to those in the healthcare industry.
- An Administrative Law Judge (ALJ) granted summary judgment in OCR's favor, upholding remedies it had imposed on a Texas hospital.
- In the Fall of 2018, OCR announced its largest monetary settlement to date.
- The agency recouped its record-breaking recovery total of $28.7 million in 2018 from 10 reported enforcement actions.

ENFORCEMENT ACTIONS

Breach settlement payments rise while other enforcement trends remain steady

Last year, OCR announced 10 resolution agreements with civil monetary penalties. A summary of these cases is outlined in the Appendix. Notably, OCR announced its largest settlement award to date when Anthem, Inc. agreed to pay $16 million following a breach of unsecured PHI affecting 79 million people. In June 2018, OCR obtained a summary judgment victory in a case alleging a Texas cancer center violated HIPAA requirements by failing to encrypt devices holding ePHI. The ALJ granted summary judgment in OCR's favor, finding that the cancer center failed to comply with requirements under the security rule to adequately secure PHI on mobile devices. The ALJ also found that OCR's remedies, which included more than $4.3 million in civil money penalties for violations due to "reasonable cause," were appropriate.[1]

This and other enforcement activity during 2018 demonstrates OCR's continued emphasis on enforcing violations of the security risk assessment and risk management requirements, which require covered entities and business associates to do the following:

1. Conduct a thorough assessment of the threats and vulnerabilities to PHI across the enterprise.
2. Implement measures to reduce known threats and vulnerabilities to a reasonable and appropriate level.

Covered entities are also cautioned to ensure that any vendor or other organization accessing or storing PHI on their behalf, particularly in electronic format or through a website, has executed a compliant BAA evidencing its agreement to safeguard PHI.

In another noteworthy development, 12 state Attorneys General[2] joined together to file suit against two Indiana-based medical IT companies alleging violations of HIPAA, pursuant to the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. § 1302(a) (HITECH), which authorizes Attorneys General to enforce compliance with HIPAA. The suit alleges, in part, that

1 The judgment has been appealed.
2 These Attorneys General are from Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska North Carolina, and Wisconsin.

defendants failed to take reasonable measures to protect their computer systems, correct known vulnerabilities, and provide timely notice of a 2015 breach. This case, pending before the Northern District of Indiana, marks the first time state Attorneys General have joined to sue under HIPAA.

While HIPAA does not provide a private right of action, covered entities experiencing a breach may be vulnerable to class action litigation under applicable state laws. In 2018, Aetna agreed to pay $17 million to settle allegations by class action plaintiffs after the company sent mailings to its members that contained large clear windows on the front, revealing identifying information and instructions related to their HIV medication.[3] In Florida, after the burglary of several unencrypted hard drives containing personally identifiable information, class action plaintiffs brought state law claims against a homecare company alleging that the defendant failed to properly secure and safeguard personally identifiable information and failed to provide timely, accurate, and adequate notice to class members that the information had been stolen. This suit is based on state law claims including negligence, invasion of privacy, and breach of implied contract.[4]

OCR guidance: emphasis on practical strategies for everyday compliance

OCR issued guidance in several noteworthy areas in 2018. As mandated by the 21st Century Cures Act, OCR issued interim guidance on the use of individual authorizations for uses and disclosures of PHI for *future* research. Additionally, in October, OCR and the HHS's Office of the National Coordinator (ONC) for Health Information Technology released an updated version of the publicly-available Security Risk Assessment (SRA) Tool that helps covered entities and business associates identify risks and vulnerabilities to ePHI. The new version of the SRA Tool provides enhanced functionality not only to help such organizations identify risks, but also document how they can implement appropriate security measures to protect ePHI.

OCR's monthly cybersecurity newsletters provided regular guidance on security controls amidst persistent cyber-threats. For instance, the May newsletter stressed a facet of security that is too-often overlooked: basic physical security measures such as protecting computers and workstations from unauthorized access and implementing low-cost physical safeguards such as privacy screens and device locks. Newsletters also highlighted other increasingly-pervasive compliance and security issues, such as avoiding cyber-extortion schemes, implementing basic cybersecurity safeguards like data encryption, and securely disposing of electronic media.

GDPR and state laws: HIPAA-related legislation spurs additional compliance efforts

2018's legislative activity, both in the United States and abroad, touched on privacy and security concepts and will propel healthcare entities to undertake compliance efforts in addition to their existing HIPAA compliance programs.

May 25, 2018 marked the compliance deadline for the European Union's General Data Protection Regulation (GDPR), which applies not only to European Union businesses, but also many companies in the United States with a global footprint. There is some overlap between GDPR and HIPAA requirements and principles, but transitioning to compliance programs consistent with both the GDPR and HIPAA is a major undertaking.

The California Consumer Privacy Act (CCPA) introduced new privacy protections and rights for consumers similar to the GDPR. Although data handled pursuant to HIPAA is technically exempt from the reach of the CCPA regulations, the rules encompass some overlapping concepts of data privacy and security. The California Attorney General is still accepting comments on the CCPA and is expected to release draft regulations and guidance in the fall of 2019. This guidance will give healthcare entities subject to the CCPA a narrow window of time to appropriately supplement their existing HIPAA-compliant privacy and security policies with additional CCPA-compatible provisions before the CCPA takes effect on January 1, 2020.

---

3 Settlement Agreement, *Beckett v. Aetna, Inc.*, 2:17-cv-03864-JS (E.D. Pa. Jan. 16, 2018). Aetna has brought suit seeking indemnity, reimbursement, contribution, and damages against claims administrator Kurtzman Carson Consultants, LLC (KCC), alleging that KCC failed to inform Aetna that it would send these mailings in a window envelope. *Aetna, Inc. v. Kurtzman Carson Consultants, LLC*, No. 2:18-cv-00470-JS (E.D. Pa. Feb. 5, 2018).

4 *Kuss v. American Homepatient Inc. & Lincare Holdings, Inc.* No. 8:18-cv-02348-EAK-TGW (M.D. Fla. Sept. 24, 2018). Defendant filed a motion to dismiss late last year, but the court has not yet ruled on it.

South Dakota and Alabama became the final two states to enact data breach legislation requiring entities to notify affected individuals of security breaches of information involving personally identifiable information. Although Alabama was the last state to implement such a law, its legislation's restrictions are formidable: Alabama joins a minority of states that not only require data breach notification, but also mandate reasonable data security measures. After Alabama's June enactment, several other states followed suit, amending their breach notification laws to include additional data security standards.[5]

Modifying the HIPAA rules: the next leg in HHS's sprint to coordinated care

In December, HHS and OCR issued a RFI seeking comments on potential modifications to the HIPAA Rules[6] focused on improving care coordination and aligning with the agency's emphasis on value-based care.[7] The RFI seeks input on four primary aspects of the HIPAA Rules:

1. OCR requests comment on ways to reduce administrative burdens and eliminate obstacles to information sharing among both healthcare and non-healthcare providers.
2. OCR seeks input on methods to encourage providers to share PHI with family members, caregivers, and others to assist in the care of those with substance use disorders and mental health illness.
3. OCR requests feedback from covered entities on the burden that accounting for treatment, payment, and healthcare operations disclosures (including through their electronic health records) would pose.
4. OCR seeks input on the administrative and economic impact of the Notice of Privacy Practices requirements, specifically those requiring healthcare providers that have a "direct treatment relationship" with individuals to make a good faith effort to obtain written acknowledgment of receipt of the Notice. Comments to the RFI were required by February 12, 2019.

LOOKING AHEAD

There is no sign that enforcement actions will slow down, particularly amidst persistent cyber-threats, including phishing attacks and ransomware. Steady consolidation across the healthcare industry can potentially make covered entities more vulnerable to lapses in security during the transition and integration phases. Careful diligence of privacy issues, security controls, and breach preparation should remain a priority for entities evaluating transactions this year.

We can also expect to see continued guidance (and possible regulatory modification) relating to the HIPAA privacy rule, as OCR seeks to balance the need for improved care coordination with protection of individual privacy. As described above, the October RFI invited ideas regarding eliminating administrative hurdles when sharing PHI to promote efficient care coordination and value-based payment. In addition, the HHS semiannual regulatory agenda, published May 9, 2018, indicated that OCR is seeking the public's input on a proposed rule that would establish a methodology for victims of data breach to share the penalties or settlements resulting from the breach. The proposal is complicated by factors such as the difficulty of proving direct damages in such cases and the possibility of encouraging frivolous suits. Lastly, OCR recently launched a campaign to encourage individuals to exercise their rights to access their PHI, and OCR continued urging covered entities to facilitate access, avoid information blocking, and increase interoperability with respect to health records. These areas of emphasis in 2018 are already being addressed in early 2019, as OCR released its proposed rule on interoperability, information blocking, and patient access on February 11, 2019. This proposed rule leads the transition, demonstrating that 2019 should be another year with plenty of HIPAA enforcement activity to monitor.

---

5 See, e.g. Louisiana (S.B. 361, Reg. Sess. (La. 2018)), Colorado, Nebraska, California.
6 The HIPAA Rules are regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191), set forth at 45 C.F.R. Parts 160-64.
7 Request for Information on Modifying HIPAA Rules to Improve Coordinated Care, 83 Fed. Reg. 64302 (Dec. 14, 2018).

APPENDIX: 2018 OCR RESOLUTION AGREEMENTS AND CIVIL MONETARY PENALTIES

ENTITY	SETTLEMENT/PENALTY	DESCRIPTION OF CONDUCT
Pagosa Springs Medical Center (PSMC)	PSMC agreed to pay $111,400 and adopt a corrective action plan.	OCR alleged that PSMC failed to terminate a former employee's remote access to a web-based scheduling calendar, which contained ePHI for more than 500 individuals. PSMC did not have a BAA in place with the former employee.
Advanced Care Hospitalists, PL (ACH)	ACH agreed to pay $500,000 and adopt a substantial corrective action plan.	ACH engaged the services of an individual claiming to be a representative of a medical billing services company, which resulted in PHI of ACH patients being posted on the website of the billing company. This breach affected more than 9,000 individuals. Allegedly, ACH never entered into a BAA with this individual and failed to conduct a risk analysis, implement security measures, or have any other HIPAA policies in place.
Allergy Associates of Hartford, PC	Allergy Associates paid $125,000 and agreed to adopt a corrective action plan.	An Allergy Associates physician disclosed the PHI of a patient, who was in a dispute with the physician, to a news reporter. Allergy Associates had instructed the physician not to respond to any media inquiries, but after the incident, it failed to discipline the physician or take any corrective action.
Anthem, Inc.	Anthem agreed to pay $16 million and take corrective actions.	A series of cyberattacks against Anthem led to the largest United States health data breach in history, exposing the PHI of nearly 79 million people. Anthem allegedly failed to implement appropriate measures to detect hackers; failed to conduct an enterprise-wide risk analysis; had insufficient procedures for regular review of system activity; failed to identify and respond to suspected or known security incidents; and failed to implement adequate controls to prevent access to sensitive information.
Boston Medical Center; Brigham and Women's Hospital; & Massachusetts General Hospital	OCR settled with each hospital and collected a total of $999,000. Each hospital also entered into a corrective action plan.	These hospitals allowed an ABC documentary television show to film on their premises. HHS stated that the hospitals did not get authorizations from the patients prior to allowing film crews on site.
University of Texas MD Anderson Cancer Center	An ALJ ordered MD Anderson to pay $4.348 million in civil monetary penalties.	The ALJ ruled in favor of OCR, finding that MD Anderson failed to comply with HIPAA by not encrypting laptops and USB drives that contained ePHI. Although MD Anderson had certain encryption policies, it experienced three breaches between 2012 and 2013 that exposed the PHI of more than 33,000 individuals because of its failure to properly implement those policies. These breaches occurred when one unencrypted laptop was stolen, and two unencrypted USB drives were lost by employees; these devices contained ePHI.
Filefax, Inc.	Filefax's receiver paid $100,000 and entered into a corrective action plan.	Between January 28 and February 14, 2015, the PHI of 2,150 individuals was disclosed when a "dumpster diver" attempted to sell medical records obtained from unsecured locations on Filefax's premises. OCR reached an agreement despite Filefax's going out of business before the investigation was complete.

ENTITY	SETTLEMENT/PENALTY	DESCRIPTION OF CONDUCT
Fresenius Medical Care North America (FMCNA)	FMCNA agreed to a $3.5 million settlement and to adopt a corrective action plan.	FMCNA filed separate breach reports regarding events involving the loss or theft of ePHI at five FMCNA facilities. The number of affected individuals at each facility ranged from 10 to 245. In its investigation, OCR found that FMCNA covered entities failed to properly conduct security risk assessments or implement reasonable and appropriate encryption procedures.
Cottage Health	Cottage Health agreed to pay $3 million and to implement a corrective action plan.	Following two reports of breaches affecting more than 62,500 patients total, OCR investigated Cottage Health and alleged that Cottage Health failed to implement security safeguards sufficient to reduce risks to PHI to a reasonable and appropriate level, as well as failed to enter into a BAA with a vendor that accessed PHI on its behalf.

AUTHORS

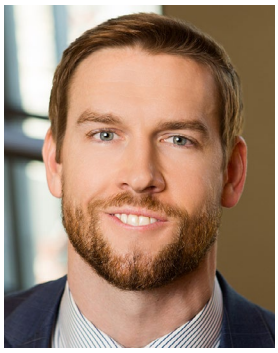
For further information on how to protect your company from a data breach, please contact one of our attorney team members.

Lisa Rivera
Member

615-742-7707
lrivera@bassberry.com

Nesrin Tift
Member

615-742-7861
ntift@bassberry.com



Jeff Gibson
Member

615-742-7749
jgibson@bassberry.com

Elizabeth Warren
Member

615-742-7719
ewarren@bassberry.com

Margaret Dodson
Associate

615-742-7712
margaret.dodson@bassberry.com

Brianna Powell
Associate

615-742-7883
brianna.powell@bassberry.com

Craig Stewart
Associate

615-742-7733
craig.stewart@bassberry.com