AMERICAN
HEALTH LAW
ASSOCIATION

2023

HEALTH CARE TRANSACTIONS

RESOURCE GUIDE

Successfully Navigate the **Transaction** Process

Coker GROUP
Business Advisors for the Healthcare Industry

Healthcare transactions are complex! **Coker's** transaction advisory experts guide you through the complexity to realize the strategic objectives of a transaction. We aim to create long-term value for all stakeholders involved in the process.

COKERGROUP.COM | 2400 LAKEVIEW PARKWAY, SUITE 400, ALPHARETTA, GA 30009 | 800.345.5829

Dealer's Choice: Paving the Way for a Successful Pick-up

Rosalind "Roz" Cordini, JD, MSN, RN, CHC, CHPC
Senior Vice President/Director of Coding & Compliance Services | Coker Group
rcordini@cokergroup.com

Jaci J. Kipreos, CPC, CPMA, CDEO, CEMC, CRC, COC
Director of Provider Audit Services | Coker Group
jkipreos@cokergroup.com

DeAnn Tucker, MHA, RHIA, CHPS, CCS, CHPC
Senior Manager | Coker Group
dtucker@cokergroup.com

Introduction

Deemed as robust, the 2022 mergers and acquisitions (M&A) market closed approximately 14% above 2021 volumes. According to Fierce Healthcare, 2022 (through 11/15) saw 2,277 healthcare deals valued at $127 billion.[1] Healthcare M&A is poised to continue to expand in 2023 with a focus, in part, on value-based care and attributed to significant levels of corporate cash and private equity "dry powder."[2]

Physicians will continue desiring to sell their practices for a variety of reasons. "There are three kinds of sellers: there is the seller who is retiring, there is the seller who is in distress, and there is the seller who is selling into growth or selling strategically."[3] Any one of these types of physician sellers will indeed consider selling their practice to a hospital/health system or private equity.

Physicians intending or desiring to sell their practice must consider many factors, including ensuring they are viewed as an attractive practice to be acquired. The following questions should therefore be considered:

1. How aligned are the practice's strategic goals with the buyer regarding market share, care delivery, and specialty?
2. Does the practice have well-documented financial information?
3. Is productivity consistent and financially beneficial across all providers in the group?
4. If retiring, is there a succession plan in place?
5. Does the practice have an electronic health records (EHR) system that can be converted to or is otherwise compatible with the buyer's EHR?
6. Does the practice have well-negotiated payer contracts?
7. Are advanced practice providers utilized to maximize efficiency?
8. Are profitable ancillary services being provided?[4]
9. Does the practice have in place an effective compliance program consistent with the size of the practice and the scope of services provided?

Given the Department of Justice's (DOJ) interest in holding private equity firms directly responsible for the actions of their portfolio companies when it comes to compliance with the False Claims Act (FCA),[5] these firms, as buyers, will be scrutinizing compliance practices and prioritizing accordingly.

An Effective Compliance Program

As early as 1991, the United States Federal Sentencing Guidelines have included the key components of a compliance program that need to be in place to mitigate punishment and reduce sentencing to a corporation. The guidelines were amended in 2004 and provide for the following:

A. Act with due diligence and the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

B. Have in place the following standards, which have become known as the "Seven Fundamental Elements" of an effective compliance program:[6]

   1. **Standards and Procedures:** Existence of standards and procedures to prevent and detect criminal conduct.
   2. **Governance and Oversight:** Designation of a compliance officer who is a high-level employee with adequate authority and resources to operate an effective compliance program.
   3. **Internal Enforcement and Discipline:** Efforts not to permit an individual to function as a high-level employee who has engaged in illegal conduct or otherwise who has acted in an unethical manner inconsistent with an effective compliance program.
   4. **Education and Training:** Effective training program on compliance and ethics to the governing body, high level, and all employees.
   5. **Monitoring and Auditing:** Have in place a program of auditing and monitoring and an anonymous reporting system for all employees to report potential or suspected compliance concerns. Periodically evaluate the effectiveness of the compliance program.

6. **Reporting:** Have in place appropriate incentives to perform in compliance and appropriate disciplinary measures that are consistently applied when compliance is not adhered to.
7. **Response and Prevention:** Appropriate response, mitigation, and program modification when noncompliance has been detected.[7]

C. Periodically assess organizational risk with respect to its compliance program.[8]

For the physician practice, the Office of Inspector General (OIG) published compliance guidelines in 2000,[9] restating the importance of the Seven Fundamental Elements and identifying pertinent risk areas applicable to physician practice groups. It also indicated that larger physician practice groups should follow the more robust compliance program measures laid out in its Third-Party Billing Company guidance.[10]

In terms of preparing to be viewed as an attractive seller from a compliance standpoint, several key areas should be considered.

Auditing and Monitoring

Proper coding is critical to maximizing revenue within a physician's practice and avoiding potentially costly repayments. In most transactions, a coding audit or revenue cycle analysis will be performed by the buyer as part of diligence and may identify one or more problematic practices, including overzealous and therefore overstated leveling of E/M services. Although rare, audits sometimes identify key concerns with significant seller liability that may be specific to the particular specialty.

The audit is the only sure method to confirm the compliance of the documentation and coding for a practice. A compliance audit does not simply verify that the codes reported were documented. There are many other areas of risk and opportunity found in a well-thought-out compliance audit. It is not uncommon to find that levels of evaluation and management services were reported with CPT codes that cannot be supported in the documentation. An audit may also show opportunities to report a higher level of service. This is an opportunity to educate providers with key strategies for applying documentation guidelines. Seller liability is often found in other areas, separate from the CPT and ICD10-CM coding. There are key areas that typically are discovered during a compliance diligence audit.

The most common findings as a result of a compliance audit include:

1. Variances in levels of E/M services reported versus documented.
2. Incorrect use of the modifier 25 when appended to an E/M service.
3. Incorrect reporting of "incident-to" services.
4. Incorrect reporting of ICD10-CM diagnosis codes.
5. Non-compliant or missing provider signatures.
6. Deficient documentation to support services reported.
7. Documentation that reflects providers copying and pasting documentation from prior encounters.

It is not uncommon for an audit to show that the documentation of evaluation and management (E/M) services either does not support the code reported or could support a higher level of service. The American Medical Association (AMA) developed new documentation guidelines that went into effect on January 1, 2021, followed by edits to those guidelines in March 2021.[11] The AMA has continued with its work in updating the guidelines for E/M codes, and on January 1, 2023, additional documentation guidelines have gone into effect.[12] With all the changes to the guidelines over the past years, providers are still experiencing a learning curve in applying all the definitions and rules that have come along with these guidelines. The need to audit the documentation of E/M services cannot be overlooked. The audit can also be performed to identify outliers within the practice. The outliers may be providers who often report much higher levels of service than their peers. The opposite may also be found. There may be a provider consistently reporting lower levels of service than their peers. Either outcome can be audited for accuracy and education. Insurance carriers typically base their requests for audits of provider documentation on claims data and the frequency of high levels of E/M services reported. This methodology can be used to determine any potential outliers and any potential need for paybacks later.

Currently, modifier 25 is under much scrutiny by all payers, not just federal programs. In 2021, the work plan created by the OIG included a specific effort to review certain claims with this modifier. The OIG titled this plan, "Audit for Dermatologist Claims for E/M services on Same Day as Minor Surgical Procedures."[13] The 25 modifier is appended to an E/M service when that service is significantly separate from a minor procedure performed during that same encounter. The provider documentation must reflect that the E/M service provided was a separate service. An auditor will compare the documentation found in the medical record to determine proper use of the modifier and will determine if the guidelines established by Medicare and the Medicare Administrative Contractor (MAC) for that region have been met. The audit will often indicate that the documentation does not support the reporting of a separate E/M service, and this has resulted in an overpayment that must be repaid.

It is difficult to identify the incorrect reporting of "incident-to" services without reviewing the documentation and signatures on the medical record. A payer will not recognize from a claim's submission that a non-physician provider (NPP) saw the patient in the office and provided the care that had been established by a physician at a prior encounter. An auditor will be able to verify that the rules of incident-to reporting were met.[14] The audit will be able to determine if the NPP saw a Medicare patient and created a new treatment plan without the involvement of a supervising physician and then reported the service under the National Provider Identifier (NPI) of a physician. An audit may also reveal that Medicare patients who are new to the practice are being seen by an NPP and the services are being reported under the NPI of a physician. Each of these scenarios will result in a payback to the Medicare program. The extent of the payback will, of course, be dependent upon the extent of the incorrect use of the incident-to rule within the practice.

An often-overlooked concern with provider documentation is the concept of copying information from a prior encounter note and bringing that information into the current encounter note without updating the information. This concept is often referred to as "cloning" or simply "copying and pasting." Per the Centers for Medicare & Medicaid (CMS), "[d]ocumentation is considered cloned when each entry in the medical record for a beneficiary is worded exactly like or similar to the previous entries."[15] In 2013, the OIG issued a report "Not All Recommended Fraud Safeguards Have Been Implemented in Hospital electronic health record (EHR) Technology."[16] This report outlines the overuse of cloning and lack of policies to address the concerns. This practice of cloning can lead to what is referred to as "note bloat." This is a medical record that includes information from other encounters that may not have even occurred during the current encounter. The result can be considered fraudulent documentation. Once an auditor identifies this activity, the integrity of the documentation begins to diminish. The auditor can determine if the pulling of information forward is being documented compliantly or if there are concerns that must be addressed.

Concerns that can be overlooked will come to light in a thorough audit. Auditors will confirm compliant signatures are being appended and can also indicate how many days it takes for a provider to sign a medical record. Although an incorrect signature should not result in a payback, it is essential to know in advance if the CMS policy on signature requirements is being followed.[17] If the practice has an internal policy that addresses when a medical record must be signed, an audit can confirm that information or reflect outliers of that policy.

Deficiencies in documentation for any type of service being reported can certainly be found during an audit. Often, providers use templates to document complex procedures or to document procedures that are frequently performed. When templates are used and the documentation is lacking key elements to support the CPT codes being reported, that can quickly result in many claims being reported with documentation that cannot support the services. Auditors will be able to identify any deficiencies in templated language and be able to identify any deficiencies in any procedure report. Deficiencies in documentation are not just related to procedures or a service. If the practice reports any injectable drugs, the exact name of the drug and dose must be documented. If providers perform any radiology or other testing in the office, the medical record must reflect the outcome of these tests. A thorough audit will identify where documentation is not supporting services that are being performed and reported.

Another area that can be identified during a complete compliance audit is the incorrect documentation of diagnoses and the incorrect reporting of ICD10-CM codes. Typically, the revenue into the practice is determined by the number or amount of relative value units (RVUs). that have been associated with a particular CPT code. However, a claim submitted with an incorrect or unspecified diagnosis code can result in a denied claim. The reviewing of the documentation in the medical record during the audit will identify any variances in either the documentation or the coding. When diagnosis codes are reported on a claim and are not supported by the documentation in the medical record, this can appear that the provider is attempting to support a higher level of E/M code by suggesting the patient had many conditions that had to be addressed. When ICD10-CM diagnosis codes are reported with a procedure and not documented, it may appear that the provider was reporting a diagnosis code that would assure medical necessity and therefore, allow a payment. An auditor will apply the ICD10-CM Official Guidelines for Coding and Reporting as established by CMS and the National Center for Health Statistics (NCHS)[18] when auditing the medical record to the claim information.

Not all audit findings are related to coding. A complete compliance audit will detect concerns that cannot be easily identified by simply reviewing claims data or reviewing a denial report. There are some variances that can only be identified by reviewing the documentation in the patient's medical record. The non-coding-related variances are often the cause of paybacks to the payer.

The outcome of any audit is opportunity. There is always an opportunity to educate staff and providers concerning correct coding, documentation, and billing. Audits provide an opportunity to identify where policies should be developed within the practice or realize it is time to perhaps audit an existing policy that is not being adhered to within the practice. Any aspect of the operations of the practice can be audited and therefore creates an opportunity for awareness and improvement. The outcome of a diligence audit may also be a decision not to pursue a practice for acquisition or a change in terms of the deal.

According to the United States Department of Health and Human Services (HHS), the government recovered four dollars ($4.00) for every dollar spent on healthcare-related fraud and abuse investigations during 2019-2021.[19] It is always beneficial to find an error before someone else finds that error. This is the biggest benefit of a complete, thorough compliance-driven diligence audit.

HIPAA Compliance

Physicians must understand and implement the requirements found in the Health Insurance Portability and Accountability Act (HIPAA) Privacy,[20] Security,[21] Breach Notification,[22] including the Omnibus Rule of 2013.[23] Since December 2000, there have been several modifications to the Privacy Rule. The largest modification was in January 2013 as part of the Omnibus Final Rule. The Security Rule was finalized in February of 2003 and was also modified by the Omnibus Final Rule (collectively, these are the "HIPAA Rules").

The HIPAA Rules were developed to protect the confidentiality, integrity, and availability of data. *Confidentiality* means that information is only accessible to authorized users. *Integrity* means safeguarding the accuracy and completeness of data and processing methods. *Availability* means ensuring that authorized users have access to data when needed.[24]

With the increased occurrence of cyber threats on healthcare organizations, the due diligence process will most certainly include a review of the seller's compliance with HIPAA including any previous violations, specifically with the requirements of the Privacy, Security, and Breach Notification rules including the Omnibus Rule from January 2013. Physicians should have in place an effective HIPAA compliance

program that includes all safeguards required to appropriately protect all protected health information (PHI).

Some commonly requested due diligence items include policies and procedures, the Notice of Privacy Practices, training materials and logs, and a list of Business Associates. Physician practices should review these documents to ensure they are up to date. The due diligence process will also focus on past privacy and security incidents and security risk analysis.

One way a physician practice can prepare for the due diligence process is to conduct its own self-assessment. In July 2018, the Office for Civil Rights updated its audit protocol.[25] The protocol is an excellent resource and can be used to help assess compliance with all three HIPAA rules including changes incorporated into them with the Omnibus Rule.

Physician Practice HIPAA Program Structure

An effective HIPAA program for the physician practice includes many important elements. The practice should appoint someone responsible for the HIPAA Privacy and Security program. This person(s) should be knowledgeable in all areas of HIPAA and the functional areas of the practice. Their primary role will be to develop, implement, and maintain the practice's policies and procedures, serve as the primary point of contact for complaints and incidents, track and document all investigations and outcomes, and manage breach notification. Monitoring compliance with established policies and procedures is continuous and can help to identify areas of noncompliance and/or risk. A complete review should also be conducted any time process or systems changes.

Often, practices will have well-known and repeatable practices in place but fail to formally document them. In addition to the required policies and procedures established by HIPAA, practices should ensure that any practice-specific policies and procedures are documented as well. Policies and procedures should be available to the practice's workforce members. They can be printed and placed in a binder for easy access or be made electronically available.

Practices must ensure that workforce members are trained on all elements of HIPAA compliance. Training should be conducted during initial onboarding and at least annually thereafter. Training should also be job specific. Training attendance can be tracked by either using a simple sign-in sheet or a more robust training program. Periodic security reminders throughout the year are an effective way to get key workforce members engaged. Reminders can be in the form of monthly emails, included as an agenda item during regular meetings, or in response to industry bulletins.

The lack of a qualified security risk analysis is the most frequent area of identified non-compliance during a diligence review. In December 2020, the Office for Civil Rights (OCR) published the results of the 2016-2017 HIPAA Audit.[26] Of the 166 Covered Entities (CE) and Business Associates (BA) the OCR audited, only a small percentage, 14% of CEs and 17% of BAs, were compliant with conducting a Security Risk Analysis (SRA) that meets the requirements outlined in the security rule (164.308(a)(1)(ii)(A)).

According to the audit, entities generally failed to identify and assess the risks to all the electronic PHI (ePHI), develop and implement an SRA policy and procedure, identify threats and vulnerabilities, review and periodically update their SRA, and conduct their SRA consistent with policies and procedures.

The OCR provides guidance on conducting a risk analysis,[27] which was adapted from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66 and NIST (SP) 800-30.[28] The scope of the security risk analysis should consider risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI. All assets that access, store, and transmit ePHI (e.g., workstations, servers, medical devices, multi-function machines, applications, etc.) should be identified. After assets are identified, all threats and vulnerabilities will need to be assessed.

In its guidance, OCR defines a threat as:

> "[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability[.]"as "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy[.]" (e.g., outdated software, unpatched systems, etc.), and a risk as "the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] . . .".[29]

Conducting a physical walkthrough to identify potential risks to paper records and verbal communications is another key component of an SRA.

SRA findings should be formally documented and shared with the physician partners. An SRA should be completed or updated at least annually due to the ever-changing landscape of information technology. Moreover, the risk analysis process should be ongoing in order for an entity to update and document its ongoing security measures.[30] New applications should be evaluated as they are implemented. The SRA findings should be used to develop a risk remediation plan that addresses the risks identified and to track risk remediation efforts.

Another common area of noncompliance relates to providing a copy of the practice's Notice of Privacy Practices on the practice's website and to its patients. HHS has provided model notices and guidance on its website.[31]

In addition to explaining how the patient's information may be used and disclosed, the notice should also explain how a patient can submit questions or complaints. All complaints should be logged including the outcome of the investigation as well as breach notification dates. Individual breach notification must be provided to patients no later than 60 days.[32] The Breach Notification Rule has very specific implementation specifications and should be reviewed when evaluating compliance. HHS provides an excellent resource on its website.[33]

Last, but certainly not least, a formal process should be in place to ensure business associates are required to safeguard PHI they create, receive, maintain, or transmit on behalf of the physician practice. The Omnibus Rule placed more requirements on business associates and

the content of the business associate agreements. A sample agreement can be found on HHS's website.[34]

Merit–Based Incentive Payment System Attestation

An often-overlooked area identified during diligence is the impact that failure to meet the security risk analysis rules has on other payment programs. Conducting an SRA is also required for participants of the CMS Merit-Based Incentive Payment System (MIPS). MIPS combines three previous programs: the Physician Quality Reporting System (PQRS), the Value-based Payment Modifier (VM) Program, and the Medicare EHR Incentive Program (Meaningful Use) into a single payment program. The MIPS quick start guide is available on their website.[35]

As a gateway element, MIPS participants must report a "yes" to the Office of the National Coordinator for Health Information Technology Direct Review Attestation, SAFER Guides, and the Security Risk Analysis measures. A physician or physician practice group participating in MIPS and realizing bonuses may be placing incentive monies at risk where there has been a failure to perform an SRA yet attested to having completed it. A strong cybersecurity program with up-to-date policies and procedures, a current security risk analysis, and remediation plan in place demonstrates the importance one has on protecting patient data.

Conclusion

Physicians desiring to sell their practice can successfully position themselves for a successful sale by performing a pre-offer review of key compliance areas specific to their practice. The existence of a compliance program with documented measures of its effectiveness could place the seller physician practice group in a buyer's top priority category.

1 Heather Landi, *Healthcare dealmaking will heat up in 2023 with plenty of corporate cash, PE 'dry powder,'* Fierce Healthcare (Dec. 8, 2022), https://www.fiercehealthcare.com/finance/expect-busy-year-healthcare-dealmaking-plenty-corporate-cash-pe-dry-powder.
2 *Id*.
3 Christopher Cheney, *How to Sell Your Medical Practice*, Health Leaders Media (Apr. 9, 2021) (quoting Barry Posner, JD, BS, a partner at Kudman Trachten Aloe Posner LLP in New York City), https://www.healthleadersmedia.com/clinical-care/how-sell-your-medical-practice#:~:text=Improving%20profitability%20is%20one%20of,buyer%20has%20sound%20financial%20standing.
4 *Practice acquisitions: What physicians need to know*, Med. Econ. (Jul. 24, 2014), https://www.medicaleconomics.com/view/practice-acquisitions-what-physicians-need-know (last visited Mar. 6, 2023).
5 Anastassia Gliadkovskaya, *The FTC and DOJ have vowed to scrutinize private equity deals. Here's what it means for healthcare*, Fierce Healthcare (Oct. 21, 2022), https://www.fiercehealthcare.com/regulatory/ftc-doj-promise-heavier-scrutiny-pe-deals-healthcare.
6 U.S. Sentencing Comm'n, *Guidelines Manual, Sentencing of Organizations*, Ch. 8B2.1 (a)(1)-(2), https://guidelines.ussc.gov/gl/%C2%A78B2.1 (last visited Mar. 6, 2023).
7 § *Id*. at (b)(1)-(7).
8 § *Id*. at (c).
9 OIG Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. 59,434 (Oct. 5, 2000), https://www.govinfo.gov/content/pkg/FR-2000-10-05/pdf/00-25500.pdf.
10 Publication of the OIG Compliance Program Guidance for Third-Party Medical Billing Companies, 63 Fed. Reg. 70,138 (Dec. 18, 1998), https://www.govinfo.gov/content/pkg/FR-1998-12-18/pdf/98-33565.pdf.
11 *CPT Evaluation and Management (E/M) Office or Other Outpatient (99202-99215) and Prolonged Services (99354, 99355, 99356, 99417) Code and Guideline Changes*, American Med. Ass'n (Mar. 9, 2021), https://www.ama-assn.org/system/files/2019-06/cpt-office-prolonged-svs-code-changes.pdf.
12 *CPT Evaluation and Management (E/M) Code and Guideline Changes (eff. Jan. 1, 2023)*, American Med. Ass'n, https://www.ama-assn.org/system/files/2023-e-m-descriptors-guidelines.pdf.
13 U.S. Dept. of Health and Human Servs., Office of Inspector Gen., *Dermatologist Claims for Evaluation and Management Services on the Same Day as Minor Surgical Procedures*, https://www.oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000577.asp (last visited Mar. 6, 2023).
14 *MLN Matters* (No. SE0441), Ctrs. for Medicare and Medicaid Servs., https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/se0441.pdf (revised Aug. 24, 2016).
15 *Electronic Health Records Provider*, Ctrs. for Medicare and Medicaid Servs. (Dec. 2015), https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/docmatters-ehr-providerfactsheet.pdf.
16 U.S. Dep't of Health and Human Servs., Office of Inspector Gen., *CMS And Its Contractors Have Adopted Few Program Integrity Practices To Address Vulnerabilities in EHRs* (Jan. 2014), https://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf.
17 *Medicare Program Integrity Manual, Ch. 3 – Verifying Potential Errors and Taking Corrective Actions, § 3.3.2.4 Signature Requirements*, Ctrs. for Medicare and Medicaid Servs., https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c03.pdf#page=44 (issued Jul. 28, 2022).
18 *ICD-10-CM Official Guidelines for Coding and Reporting FY 2022*, Ctrs. for Medicare and Medicaid Servs., https://www.cms.gov/files/document/fy-2022-icd-10-cm-coding-guidelines-updated-02012022.pdf (updated Apr. 1, 2022).
19 U.S. Dep't of Justice and U.S. Dep't of Health and Human Servs., *Annual Report of the Departments of Health and Human Services and Justice, Health Care Fraud and Abuse Control Program FY 2021* (July 2022), https://oig.hhs.gov/publications/docs/hcfac/FY2021-hcfac.pdf.
20 45 C.F.R. 164.500 (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.500.
21 45 C.F.R. 164.302 (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.302.
22 45 C.F.R. 164.400 (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D.
23 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566 (Jan. 25, 2013), https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/FR-2013-01-25.pdf.
24 45 C.F.R 164.304 (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.304.
25 U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Audit Protocol – Updated July 2018*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html (last reviewed Aug. 17, 2018).
26 U.S. Dep't of Health and Human Servs., Office for Civil Rights, *2016-2017 HIPAA Audits Industry Report* (Dec. 2020), https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.
27 U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (July 14, 2010), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.
28 Matthew Scholl et al., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, Nat'l Inst. of Standards and Tech. (Oct. 2008), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.
29 U.S. Dep't of Health and Human Servs., *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (July 14, 2010), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.
30 45 C.F.R. 164.306(e) (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306 and 164.316(b)(2)(iii) (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316.
31 U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Model Notices of Privacy Practices*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html (last reviewed Apr. 8, 2013).
32 45 C.F.R. 164.404(b) (2023), https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D/section-164.404.
33 U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last reviewed July 26, 2013).
34 U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Business Associate Contracts, SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS* (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (last reviewed June 16, 2017).
35 U.S. Dep't of Health and Human Servs., Quality Payment Program, *Participation Options Overview*, https://qpp.cms.gov/mips/overview (last visited Mar. 6, 2023).

Educating and Connecting the Health Law Community

1099 14th Street, Suite 925, Washington, DC 20005
www.americanhealthlaw.org
info@americanhealthlaw.org

Printed in the U.S.A.