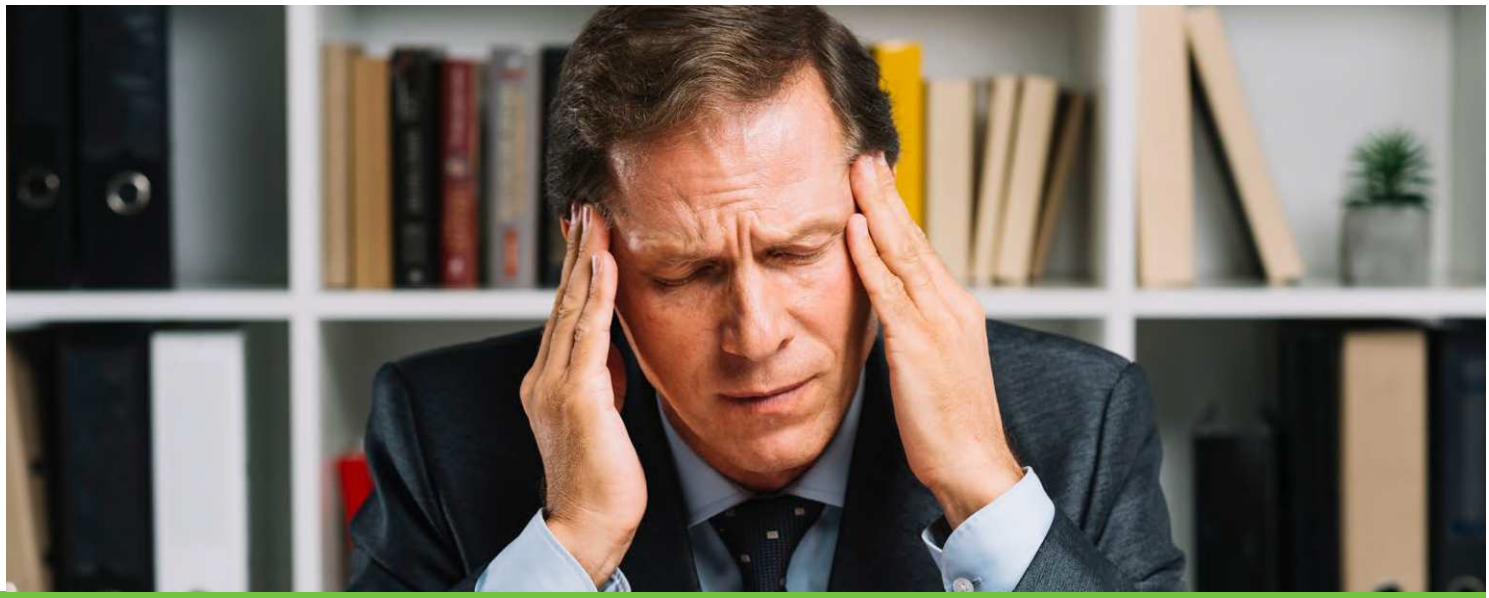

Occupational Health Services and HIPAA: Do I Really Need to Care?

By Roger Shindell, MS, CHPS, CISA, CIPM

Anyone working with medical information quickly begins to hear about the need to maintain HIPAA practices for privacy and security to maintain the confidentiality of the medical information. When it comes to occupational health services, HIPAA is not the overriding regulation that governs the protection and disclosure of the occupational health record (OHR). Rather, a variety of other federal and state regulations govern the protection and disclosure of the OHR. HIPAA does come into play as a well developed and accepted framework to maintain the privacy and security of the OHR. As such, HIPAA should be considered the "go-to" framework for the protection of the OHR.

HIPAA is fraught with misunderstanding and misconception. How significant is the regulation to your occupational health practice? HIPAA is not going to be a major regulatory factor in your occupational health services, but before you take too much comfort in that statement, first you are going to need to understand why this is so. While technically you have little to fear from compliance with HIPAA, you are still going to consider HIPAA and implement a privacy and security program that will comply with the regulations - more on that later.

To make this easy, at least on the surface, HIPAA is not going to apply to your occupational health practice unless you are a covered entity. OSHA rules, not HIPAA regulations, govern the access and release of information relating to OHR. These are records maintained by employers and/or their contracted occupational health service providers. Though fairly straight forward, some confusion may come, because the disclosure rules under OSHA are similar to HIPAA. Additionally, some organizations may perform services that may fall under HIPAA, while also performing services that fall under OSHA. In these cases, care must be taken to isolate and segregate these services and their records.

To determine when HIPAA applies to the records and/or your services, you must first determine if the record in question is protected health information (PHI) or an OHR. This is determined by what information is in the record and who has collected and owns the information.

PHI is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations, and/or payment for healthcare services. PHI refers to records in paper format and, in the case of electronic health information, ePHI. PHI includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage.

The occupational health medical record is the occupation-related, chronological, cumulative record, regardless of the form or process by which it is maintained (i.e., paper document, microfiche, microfilm, or automatic data processing media). The OHR includes information about health status documented on an employee, including personal and occupational health histories as well as the opinions and written evaluations generated in the course of diagnosis, employment-related treatment, and examination by healthcare professionals and technicians. The definition includes employee exposure records, occupational illness, and accident or injury records.

When a healthcare provider chooses to provide occupational health services, the contractual relationship with the employer will determine ownership of the record as well as how the record is created and

maintained. A couple of examples regarding ownership and disclosures of OHRs will illustrate some potential complications.

- **SCENARIO 1:** A healthcare provider renders occupational health services at a clinic site. Health records are created and maintained as PHI. Copies of the PHI are provided to the employer only upon authorization by the patient. In this scenario, the provider owns the record and is subject to HIPAA and all other pertinent federal and state regulations governing patient health records. The employer maintains copies as part of the employee's human resource employee health records and is not subject to HIPAA but is subject to OSHA and all other federal and state regulations governing employee health records.
- **SCENARIO 2:** The healthcare provider renders occupational health services at the employer's site. All records of encounters are maintained by the employer as employee health records. The provider does not maintain PHI or health records. In this scenario, the employer owns the employee's occupational health record and is subject to OSHA and all other federal and state regulations governing employee health records. The healthcare provider has no further ownership or responsibility for protected health records.
- **SCENARIO 3**: A healthcare provider renders occupational health services to external entities under contract and additionally provides the same type of services through its employee health department. However, occupational health services rendered by the healthcare provider for its own employees in its role as an employer are not covered by HIPAA but are subject to OSHA and all other federal and state regulations governing employee health records.

Given the discussion so far and the examples presented above, why do we really care about HIPAA? First and before I answer that question, let's look at the regulations the occupational health practitioner needs to be concerned about.

The Equal Employment Opportunity Commission Office of Legal Counsel states, "accessing an individual's medical records directly is no different from asking an individual for information about current health status, which the Commission considers a request for [disability or] genetic information where it is likely to result in the acquisition of such information, particularly family medical history." Therefore, employers must respect the confidentiality of medical information maintained for employment purposes.

Additionally, the EEOC's opinion letter makes clear employers must ensure personal health information about applicants or employees cannot be accessed, except under the circumstances and to the extent permitted under ADA and GINA.

Healthcare providers and health plans, both in their capacity as HIPAA-covered entities and in their capacity as employers, need to ensure appropriate separation and access controls exist with respect to both PHI and employment/occupational health information maintained in paper or electronic form. Failure to do so could result in potential liability under ADA and GINA, as well as the more typical risk of a "breach" under HIPAA's requirement to notify patients when their medical records have been accessed or acquired in an unauthorized, or illegal, manner.

The Federal Trade Commission takes the position that vendors of personal health records and related entities are to notify consumers following a breach involving unsecured information. If a service provider to one of these entities has a breach, it must notify the entity, which in turn must notify consumers. The final rule also specifies the timing, method, and content of notification, and, in cases of certain breaches involving 500 or more people, requires notice to the media. Additionally, it interperates the FTC Act sections on fraud and abuse and deceptive practices to include the expectation of privacy for organizations gathering highly sensitive content combined with identifiers of individuals and places the burden on both the vendor and user of the electronic health record system (EHR), believing the individual whose information is stored in the system likely believes communications are private.

Finally, professional codes of ethics address the need for privacy and security of the OHR. For example, the American College of Occupational Health and Environmental Medicine's (ACOEM) code of ethical conduct states, "Keep confidential all individual medical, health promotion, and health screening information, only releasing such information with proper authorization." The American Association of Occupational Health Nurses, Inc.'s (AAOHN) code of ethics states, "… Maintains the confidentiality of personal and health information of clients and protects the privacy rights of workers' personal identifiable information as prescribed by local, state, federal and international guidelines, policies regulations and laws.… develops and routinely updates written policies and procedures guiding access, release, transmission, and storage of personal and health information, including electronic records."

As discussed, HIPAA is not going to be your primary regulatory concern. There is a variety of federal and state regulations you will have to satisfy specific to the OHR. The questions become how are you going to comply with the wide variety of these regulations and what kind of privacy and security framework are you going to implement to address the regulations you need to comply with? That is where HIPAA comes in. HIPAA is the most robust and complete set of safeguards addressing physical, technical, and administrative vulnerabilities faced by medical records. As a framework, it is straightforward and well accepted. Each of the alternate regulations discussed requires you to comply with their unique requirements. Implementing a privacy and security program based on the requirements of HIPAA will provide you with the foundation of a privacy and security program that will cover with a few modifications each of the regulations and standards of practice discussed above. The objective of your program should be first to give you and your clients the confidence you are doing all you can to keep their information as private, safe, and secure as possible. Additionally, you are providing both an insurance policy and an affirmative defense to the consequences that will come when you have that inevitable breach of the OHR.

Roger Shindell, MS, CHPS, CISA, CIPM

Founder and CEO, Carosh Compliance Solutions