The Privacy and Security of Occupational Health Records

The Occupational Safety and Health Administration (OSHA) defines an "occupational medical record" as an 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 occupational medical record 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.

The terms occupational medical record, occupational health record, and employee health record are often used interchangeably. For the purposes of this practice brief it will be referred to as the occupational health record (OHR). This practice brief will discuss a variety of issues related to OHRs, including privacy and security principles as well as content and record management practices for the healthcare provider. For the purposes of this practice brief, the term "healthcare provider" includes hospitals, ambulatory, surgery centers, physicians, clinics, and other healthcare providers.

The management of OHRs has always presented challenges to healthcare providers and health plans. Those challenges have multiplied for leaders in health information management (HIM) and privacy and security as regulatory compliance directives and technological advances further emphasize the need to balance access with privacy and security.

Some of the challenges of managing OHRs include understanding the different regulations that govern these records including when and how to apply them, ownership of the records, when and what information may be shared with whom, and how to appropriately manage these records when they can be part of an individual's employee health record as well as their patient health record. Additionally, the management of these records can be further complicated by inclusion in health information exchanges (HIEs), patient portals, and required external reporting repositories, etc.

Occupational health providers face the unique challenge of serving multiple simultaneous clients:

1. Employer
2. Employee/patient
3. Employer's insurance carrier, self-insured administrator, or workers' compensation carrier
4. Employee's healthcare provider

The provider may need to continuously adjust to understand their responsibility for each role performed, depending on the client they are serving at the time.

The HIM and privacy and security professionals who support these providers and health plans are tasked with understanding the various regulations and how they apply to the different roles and relationships between employee and occupational health provider or health plan. This understanding is important in order to implement effective compliance measures to protect these unique records.

Defining Occupational Health Records

The occupational health record must meet certain legal and regulatory requirements. Whether the OHR is created by the healthcare provider or the employer, record keeping should follow the same general principles of other health and business records:[1]

- Documentation in the record should clearly identify the individual to which it pertains.
- Entries should be made in the ordinary course of business, at or near the time of encounter by individuals authorized to make entries.
- Entries should be legible, signed, dated, and timed.
- Documentation should be physically or electronically secured to protect against unauthorized access, use, and/or disclosure.

Content of the Occupational Health Record

The content of the OHR can vary and may include, but is not limited to:

1. Results of physical examinations
2. X-ray, laboratory, and other diagnostic study reports (including EKG, pulmonary function results, and audiograms)
3. Acute care entries and progress notes (an additional separate acute care register is often also kept)
4. Immunization records where required or recommended for job performance or condition of an employment
5. Occupational and medical history
6. Hazard exposure record (i.e., bodily fluids, chemicals, or other substances)
7. Health programs participation record
8. Informed consent forms and authorizations for disclosure of information
9. Documentation of refusals to undergo examination, testing, and program participation
10. Workers' compensation and insurance medical records such as the Family and Medical Leave Act
11. Progress notes for rehabilitation
12. Wellness assessments and activity records
13. Consultant reports:
    a. Pre-employment and employment physical
    b. Immunization records where required or recommended for job performance or condition of an employment
    c. Records of exposure to bodily fluids, chemicals, and other substances
    d. Medical complaints related to workplace injuries and illnesses
14. Medical certifications and re-certifications
15. Substance abuse screening
16. Independent medical evaluation

There are other OSHA-specific standards such as exposure records, medical surveillance records, and other activities relating to occupational safety that could impose additional maintenance and reporting to OSHA and the employees. More information on OSHA standards can be obtained at www.OSHA.gov.

OHR managers may need to assess whether documentation properly belongs in the OHR. Some challenges encountered might include:

- Determining if the injury or illness is work-related and capturing the documentation of that injury or illness (i.e., injuries occurring when employees are traveling on official business or working at home)
- Clearly distinguishing between occupational health records controlled by employers and non-occupational health records controlled by the patient or employees
- Designing an electronic health record system that is able to manage and segregate different types of health record systems with differing rules of access, use, and disclosure as needed
- Under certain conditions, OHR may crossover to be included in the general health record (for example, immunization records that may reside in the OHR as well as the patient's general health record)

While OHRs may include some of the same information as the general record, it is important to remember that they must remain independent and distinct as outlined by OSHA. As the records evolve to electronic format, significant attention to role-based access frameworks should be made.

Ownership, Access, and Disclosure of OHRs

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. Examples of delivery scenarios may include:

- **Scenario 1:** A healthcare provider renders occupational health services at a clinic site. Health records are created and maintained as protected health information (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.
- **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 occupational health record (employee 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. This scenario is beyond the scope of this practice brief. Refer to www.osha.gov for further guidance.

A healthcare provider may render occupational health services to external entities under contract and additionally provide 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.[2] Throughout the December 2000 preamble to the HIPAA Privacy Rule, the Department of Health and Human Services repeatedly stated that the privacy rule does not apply to employers, nor does it apply to the employment functions of covered entities-that is, when they are acting in their role as employers.[3] Hence these records are maintained in accordance with the OSHA rules. When determining which rules to follow, one must ask whether the healthcare provider is providing services as an occupational health service provider to its employees or another external entity's employees. Each organization must develop an effective registration process to accurately identify these individuals to distinguish them from other types of patients.

While the employer owns the physical OHR, the employee has certain rights to access, inspect, copy, and control the use and disclosure of the information contained within their health records.[4,5,6] Particular circumstances may vary for access to medical and exposure records. Refer to the provisions of the OSHA standard for specific information and requirements.

Ownership of aggregated data is different. Such data should be de-identified and addressed in the contract between the employer and the occupational healthcare provider. An example may include the employer contracting with the healthcare provider to conduct health or wellness assessments of its employees in order to determine if a cooperative health wellness program could be beneficial for the employee group. The aggregated data from the assessments would be owned by the receiving party-the employer. PHI may only be disclosed with the employee's authorization.

OHR Legal Aspects, Disclosure of Information

An occupational healthcare provider may disclose information to the employer, the patient, the government, or other third parties. Agencies such as OSHA, the US Department of Transportation, or other state equivalents and laws such as the Americans with Disabilities Act and the Family and Medical Leave Act may require employers to submit medical information regarding their employees. As with analyzing any potential use or disclosure of protected health information, attention immediately turns to HIPAA and the applicability of the corresponding privacy and security rules. Along with the privacy and security rules, HIPAA applies only to covered entities engaged in covered transactions. In addition to HIPAA, many states have adopted state-specific laws that must be reviewed prior to any disclosure of PHI. Other federal laws must also be addressed, such as the Substance Abuse Confidentiality Regulations.

Under HIPAA, an occupational health provider who is a covered entity and transmits PHI electronically (which includes faxing information from a paper or hybrid system) must abide by the HIPAA rules addressing electronic transmissions as defined by the HIPAA regulation 45 CFR 160.103. There may be limited circumstances where a standalone occupational health provider may not be a covered entity under HIPAA. Prior to releasing information, an occupational healthcare provider should consider the following questions:

1. Does the disclosure involve individually identifiable health information or PHI?
2. When required, has the patient signed a valid authorization or consented to the disclosure?

3. Is it a permitted or required disclosure?
4. Does the minimum necessary standard apply?
5. Do other federal or state laws apply?

Valid Authorizations and Disclosures

Healthcare providers with limited exceptions must release information pursuant to a valid HIPAA authorization. However, the healthcare provider is also permitted to disclose information to the employer, provided the patient has either given consent or has been given an opportunity to agree or object. In this case, the disclosure must meet the requirements set out in HIPAA regulation 45 CFR 164.512:

- The patient must be a past or present member of the employer's workforce
- The purpose of the information being disclosed is:
    - To conduct an evaluation relating to medical surveillance of the workplace; or
    - To evaluate whether the individual has a work-related illness or injury

Information may also be released if it is necessary to comply with federal or state law.

Minimum Necessary Standard, Federal and State Laws

With the exception of disclosures that are required by law, the healthcare provider needs to "make reasonable efforts" to ensure that only the minimum amount of information is disclosed to achieve the intended purpose. This is important when the healthcare provider is conducting an evaluation for a specified limited purpose and the patient discloses other unrelated PHI.

Take the following scenario as an example. "Patient A" presents to the healthcare provider for an employer-required fitness exam. The provider has been requested by the employer to complete a short exam form and indicate whether the employee is cleared for duty (the patient has signed a consent form allowing for this limited information to be disclosed to the employer). Prior to the examination, the provider has the patient complete a short medical history and review of systems form. On this form the patient discloses that he has an unrelated chronic illness for which he is receiving treatment. The condition is currently under control and does not affect his ability to perform job-related functions. In this case, the provider should only release the specific information requested on the short exam form. However, specific state laws may require the covered entity to release other information as well. The provider should not disclose information related to the chronic condition unless required by law, or if the provider believes there is an imminent threat to public safety.

Verifying Patient and Requestor Identity

The healthcare provider must verify the identity of the person requesting the information and verify the authority of the person or entity to have access to this information. Strong practices include asking for photo identification or comparing a signature to a prior one. The healthcare provider may act in good faith and may not be required to follow any specific requirements to verify a patient's identity. The importance of patient identification, options for verifying this information, and alternatives to using social security numbers are discussed in greater detail in the AHIMA practice brief "Limiting the Use of the Social Security Number in Healthcare."[7]

Best Practice Recommendations

OHRs require the same protections as any health record containing confidential personal and health information. Whether the records exist in a paper or electronic format, they must be stored in a secured area free from unauthorized access, use, or disclosure. Providers and organizations must ensure compliance with regulations and requirements through effective policies and procedures. Staff handling OHRs should receive training upon employment and continuously thereafter regarding policies and procedures associated with safeguarding the privacy and security of OHRs. At a minimum, the following practices must be considered:

- Role-based access and enforcing unique user logins and strong passwords will help to ensure the safety of electronic information, allowing access only by authorized users.
- Routine access audits for appropriateness should be ongoing, and appropriate technical safeguards such as encryption and firewalls should be in place.
- Establish administrative, technical, and physical safeguards, such as locked file cabinets, shred bins, and secured fax locations.
- Random review of OHRs must occur to ensure accurate and complete documentation in accordance with health record regulations and requirements. Incomplete items should be referred back to the appropriate provider for prompt completion. Additionally, documentation must be reviewed to ensure no misfiled entries have occurred.
- Routine review of the federal and state privacy and security regulations is necessary to evaluate how changes may impact occupational health practices and to serve as a stimulus for updating policies, procedures, and staff education for the occupational health organization.

Another factor that must be accounted for is the arrangement details a provider enters into with an employer regarding OHRs. Prior to entering into an arrangement, the employer should identify and clarify the following with the occupational healthcare provider:[8]

- How are the services being provided? Are they provider-based, or provided through another contracted service?
- How is the provider being compensated? Fee-based patient encounter claim or compensated flat rate for services provided with no individual claims or encounter fees?
- What potentially “intersecting” roles exist with other entities (i.e., health plan)?
- What privacy considerations will be shared with the patient?
- Who owns the health records or health information?
- What federal and state regulations impact the creation, maintenance, retention, and disposal of the health records?
- Who can access the health information without patient/employee authorization?
- Who can disclose the health record/health information to others?
- How will conditional authorizations be handled? For instance, when a healthcare provider contracts with an employer to provide services (i.e., pre-employment

physicals), the authorization obtained is a "conditional" one where the service will not be performed unless the authorization is signed.

What is Not an Occupational Health Record?

Defining the OHR is not easy and can be cause for confusion. However, there are certain types of information that can be identified as not being a part of the OHR. This should be clearly understood by all providers before any occupational health services begin.

The first type of information pertains to environmental hazard records. These records typically are not a part of the OHR. These records include site visit reports, hazard monitoring results, worksite health and safety committee reports, and accident investigation files. They are normally produced and maintained by the employer's safety or hygiene staff, but in a small company they may be the responsibility of designated operations personnel. Environmental hazard records or reports may trigger the need to refer an employee to an occupational health services entity or the employee health department.

In addition to environmental hazard records, the following also are not considered part of the occupational health record:

- Employee assistance program records
- Alcohol, drug, or substance abuse records
- Patient health records that are non-work related

The second type of information not to be included in an OHR is any type of record related to workers' compensation. The Federal Employees' Compensation Act (FECA) distinguishes between the use of health information for injury reporting and safety management, management of the clinical care of employees, and the administrative management of workers' compensation claims. The use of the information used in the filing of workers' compensation claims is restricted to the employees filing the claims, their supervisors, and workers' compensation personnel. Although the health records of an employee who elects to obtain treatment in occupational health may be used by clinicians in the provision of medical care, this information may not be accessed by supervisors, human resource managers, or other individuals not designated as workers' compensation staff unless the individual provides a written authorization for such use of the information.

Notes

1. Fahrenholz, Cheryl G. and Ruthann Russo. *Documentation for Health Records.* Chicago: AHIMA Press, 2009.
2. Brandt, Mary. "HIPAA Q&A: HIPAA and occupational health." *HIM-HIPAA Weekly Advisor*. June 7, 2010. http://www.hcpro.com/HIM-251973-866/HIPAA-QA-HIPAA-and-occupational-health.html.
3. Bricker and Eckler. "Exclusion for Employment Records." http://www.bricker.com/services/resource-details.aspx?resourceid=262.
4. LaTour, K., and S. Eichenwald-Maki. *Health Information Management-Concepts, Principles, and Practice,* Second Edition. pp. 251-252. Chicago: AHIMA Press, 2006.

5. American Medical Association. “Council on Ethical and Judicial Affairs Opinion #7.02.” Code of Medical Ethics of the American Medical Association. 2006. https://catalog.ama-assn.org/MEDIA/ProductCatalog/m1100080/AMA%20Code%20of%20Ethics.pdf.
6. Roach, William H. *Medical Records and the Law*. Sudbury, MA: Aspen Publishers, 1994, pp. 96-97.
7. AHIMA. “Limiting the Use of the Social Security Number in Healthcare.” *Journal of AHIMA* 82, no.6 (June 2011): 52-56.
8. HIPAA Collaborative of Wisconsin. “Management of Occupational Health Records Whitepaper.” September 2007. http://www.hipaacow.org/home/home.aspx.

References

AHIMA. “Management Practices for the Release of Information.” *Journal of AHIMA* 83, no.2 (February 2012).

Department of Veterans Affairs. *“Occupational Health Record-Keeping System.”* VHA directive. April 11, 2012. http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=2505.

Guidotti, Tee et al., eds. *Occupational Health Services: A Practical Approach,* 2nd ed. Oxon: Routledge, 2012, pp. 176-177.

“Standards for Privacy and Individually Identifiable Health Information; Final Rule.” *Federal Register* vol. 67, no. 157 (August 14, 2002). http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrulepd.pdf.

OSHA. *OSHA Recordkeeping Handbook: The Regulation and Related Interpretations for Recording and Reporting Occupational Injuries and Illnesses.* OSHA 3245-03R, 2006. http://www.osha.gov/Publications/recordkeeping/OSHA_3245_REVISED.pdf.

Prepared By

Benjamin Burton, JD, MBA, RHIA, CHP, CHC
Carey Cothran, CHP
Nancy Davis, MS, RHIA
Julie Dooling, RHIT
Rose Dunn, MBA, CPA, RHIA, CHPS, FACHE
John Jensen, CHPS, CIPP/US
Godwin Odia, PhD, NHA, RHIA, CAPT, USPHS
Angela Dinh Rose, MHA, RHIA, CHPS
Mariela Twiggs, MS, RHIA, CHP, FAHIMA

Acknowledgements

Jeff Biedermann, JD
Ann Botros, PhD, RHIA
Becky Buegel, RHIA, CHP, CHC
Debbie Case, MBA, RHIT
Kim Turtle Dudgeon, RHIT, HIT Pro-IS/TS, CMT

Joe D. Gillespie, MHS, RHIA, CHPS
Elisa R. Gorton, MAHSM, RHIA, CHPS
Christina Grijalva, RHIA
Michele Kruse, MBA, RHIA, CHPS
Kelly McLendon, RHIA, CHPS
Mary Poulson, MA, RHIT, CHC, CHPC
Nancy Prade, RHIA
Margaret Schmidt, RHIA, CHPS
Diana Warner, MS, RHIA, CHPS, FAHIMA
Lou Ann Wiedemann, MS, RHIA, FAHIMA, CDIP, CPEHR

Source: **http://library.ahima.org/doc?oid=106321#.X74HBs1Kg2w**

Article citation:
AHIMA. "The Privacy and Security of Occupational Health Records" *Journal of AHIMA* 84, no.4 (April 2013): 52-56.