BILLING CODE: 4510-26-P

DEPARTMENT OF LABOR

Occupational Safety and Health Administration

29 CFR Part 1913

[Docket No. OSHA-2020-0005]

RIN 1218-AC95

Rules of Agency Practice and Procedure Concerning Occupational Safety and Health Administration Access to Employee Medical Records

AGENCY: Occupational Safety and Health Administration (OSHA); Labor.

ACTION: Final rule.

SUMMARY: OSHA is issuing a final rule to amend the regulation addressing the rules of agency practice and procedure concerning OSHA access to employee medical records. The final rule transfers the approval of written medical access orders (MAO) from the Assistant Secretary for Occupational Safety and Health (Assistant Secretary) to the OSHA Medical Records Officer (MRO) and makes the MRO responsible for making determinations regarding inter-agency transfer and public disclosure of personally identifiable medical information in OSHA's possession.

DATES: This final rule is effective on [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: In accordance with 29 U.S.C. 2112(a)(2), OSHA designates, Mr. Edmund C. Baird, Associate Solicitor of Labor for Occupational Safety and Health, Office of the Solicitor, Room S-4004, U.S. Department of Labor, 200 Constitution Avenue, NW, Washington, DC 20210, to receive petitions for review of the final rule.

FOR FURTHER INFORMATION CONTACT:

Press inquiries: Mr. Frank Meilinger, OSHA, Office of Communications; telephone: (202)-693-1999; email: *Meilinger.francis2@dol.gov*.

General and technical information: Dr. Michael Hodgson, Director, OSHA Office of Occupational Medicine and Nursing; telephone: (202) 693-1768; email: *hodgson.michael@dol.gov*.

SUPPLEMENTARY INFORMATION: The final rule also amends § 1913.10 to clarify that a written MAO does not constitute an administrative subpoena, eliminates outdated requirements for the removal of direct personal identifiers when OSHA personnel review medical information away from a worksite, and establishes new procedures for the access and safeguarding of personally identifiable employee medical information in electronic form. The revisions to § 1913.10 in the final rule will increase employee privacy and enhance OSHA's ability to safeguard personally identifiable medical information.

Table of Contents

I. Background

A. Introduction

In order to carry out its statutory obligations, OSHA often reviews employee medical records. For example, OSHA may need to review employee medical records during a compliance inspection to determine whether an employer is in compliance with OSHA standards and regulations, or to verify that an employer has taken steps to correct existing violations. Access to employee medical records may also be necessary during inspections to determine the effectiveness of voluntary employer safety and health programs. OSHA also reviews medical records when gathering information during agency rulemaking to develop or revise occupational safety and health standards.

Several OSHA standards and regulations mandate medical records access, including 29 CFR 1910.1020, Access to Employee Exposure and Medical Records, which sets forth procedures by which exposure and medical records can be accessed by employees, their designated representatives, and OSHA. This regulation, which applies to employers with employees exposed to toxic substances and harmful physical agents, provides OSHA representatives with prompt access to employee exposure and medical records and to analysis thereof using exposure or medical records. See 29 CFR 1910.1020(e)(3). In addition, several of OSHA's substance-specific standards include provisions for OSHA access to employee medical records. (e.g., 29 CFR 1910.25(n)(4) (Lead), and 29 CFR 1910.1028(k) (Benzene)).

In many instances, OSHA must examine and copy employee medical information in personally identifiable form. Personally identifiable employee medical information as defined by 29 CFR 1913.10(b)(2) means employee medical information accompanied by either direct identifiers (name, address, social security number, payroll number) or by information which could reasonably be used in particular circumstances indirectly to identify specific employees (e.g., date of birth, race, sex, date of initial employment, job title). An employee medical record may include individual health histories as well as medical opinions and evaluations generated during diagnosis, physical examinations, or medical treatment by a health care professional.

Because of the substantial personal privacy interests involved, OSHA authority to access personally identifiable employee medical information is exercised only after the agency has made a careful determination of the need for the information, and only when appropriate safeguards are in place to prevent unauthorized access. Once this information is accessed, OSHA examination and use is limited to only that information needed to accomplish a relevant statutory purpose. Also, personally identifiable employee medical information is retained by OSHA only for so long as needed to accomplish the purpose for access, is kept secured while being used, and is not disclosed to other agencies or members of the public except in narrowly defined circumstances. In addition, the examination and use of personally identifiable employee medical information is limited to only OSHA personnel with a need to review such information.

This rule is not an Executive Order (EO) 13771 regulatory action because this rule is not significant under EO 12866. Pursuant to the Congressional Review Act (5

U.S.C. 801 et seq.), the Office of Information and Regulatory Affairs designated this rule not a 'major rule', as defined by 5 U.S.C. 804(2).

B. OSHA's Regulation at 29 CFR 1913.10

On May 25, 1980, OSHA issued a final rule entitled Rules of Agency Practice and Procedure Concerning OSHA Access to Employee Medical Records (45 FR 35284). The final rule was developed and published in concert with the promulgation of 29 CFR 1910.1020, Access to Employee Exposure and Medical Records (45 FR 35212). During the rulemaking, there was universal agreement that if OSHA obtained access to employee medical records, the access should be accompanied by stringent internal agency procedures to preclude abuse of personally identifiable medical information. Provided these procedures were established, many participants in the rulemaking endorsed OSHA access to employee medical records without the consent of the employee for occupational safety and health purposes (see 45 FR 35218).

Except as provided in 29 CFR 1913.10(b)(3) through (6), the rules of agency practice and procedure apply to all requests by OSHA personnel to obtain access to records to examine and copy personally identifiable employee medical information, whether or not access is mandated by 29 CFR 1910.1020. Among other things, the regulation at 29 CFR 1913.10 establishes certain responsibilities for specific OSHA officials when the agency accesses personally identifiable employee medical information. The regulation also includes provisions addressing the internal use of employee medical records by agency personnel, as well as requirements for inter-agency transfer and public disclosure of such records. The regulation includes security procedures for the use and storage of employee medical records while in the agency's possession. Finally, the

regulation sets forth internal agency requirements for the retention and destruction of records.

A key provision set forth in § 1913.10 is that, with few exceptions, each request by an OSHA representative to examine or copy personally identifiable employee medical information must be made pursuant to a written access order. The written access order is an authorization for specific OSHA personnel to examine or copy personally identifiable employee medical information contained in records held by an employer or other record holder. The rules of agency practice and procedure in § 1913.10 make clear that each written access order must state the statutory purpose for which access is sought, a general description of the type of employee medical information that will be examined and why there is a need to examine personally identifiable information, whether the medical information will be examined on-site, what type of information will be copied and removed off-site, and the anticipated time during which OSHA expects to retain the employee medical information in personally identifiable form.

In order to enhance employee privacy, and clarify certain provisions, OSHA has determined that it is necessary to revise its regulation at § 1913.10. For example, OSHA's previous regulation at § 1913.10 used the term "written access order." However, this final rule revises the regulatory text to include the more commonly used term "medical access order" or "MAO."

The final rule also amends the regulation at 29 CFR 1913.10 to transfer certain responsibilities from the Assistant Secretary to the OSHA Medical Records Officer (MRO). Specifically, the MRO will now be responsible for the overall administration and implementation of the procedures contained in § 1913.10. These new responsibilities

include making determinations regarding (1) OSHA access to personally identifiable employee medical information pursuant to a MAO, and (2) inter-agency transfer and public disclosure of personally identifiable employee medical information. The final rule also transfers responsibility from the Assistant Secretary to the MRO for issuing written directives that authorize OSHA compliance personnel to review certain information without obtaining a MAO.

The final rule clarifies that a MAO does not constitute an administrative subpoena, and eliminates requirements for the removal of direct personal identifiers when OSHA personnel review medical information away from a workplace. The deletion of requirements for the removal of direct personal identifiers will be offset by new provisions designed to strengthen employee privacy. Finally, the final rule establishes new internal OSHA requirements, based on existing agency policy, for the access and safeguarding of personally identifiable employee medical information maintained in electronic form.

The procedures set forth in § 1913.10 are internal agency procedures and do not affect employer compliance with OSHA requirements. Employers and employees will benefit from the revisions to § 1913.10 in several ways. First, since the process for determining whether there is a need for OSHA to review employee medical information will be more efficient, employers will know sooner if such a review is authorized at their worksite. Second, the elimination of the outdated requirement to remove direct personal identifiers before taking medical information off-site for review will reduce the amount of an employer's time and physical space needed by OSHA personnel when they visit a specific workplace. Third, the revisions will benefit employees because the procedures in

§ 1913.10 to protect the security and privacy of employee medical records will be strengthened, especially with regard to medical information in electronic form. Fourth, the elimination of the requirement to remove direct personal identifiers before taking medical information off-site will enhance employee privacy because the removal process always carries with it the possibility that medical information will be misidentified or mislabeled, which could result in unauthorized staff mistakenly reviewing that information. Finally, deletion of the time-consuming de-identification procedures will mean that authorized OSHA personnel can conduct follow-up consultations with employees about their health more quickly.

The notice and comment rulemaking procedures of 5 U.S.C. 553 of the Administrative Procedure Act (APA) do not apply to "interpretive rules, general statements of policy, or rules of agency organization, procedure, or practice." 5 U.S.C. 553(b)(A). The provisions in 29 CFR 1913.10 are rules of agency procedure and practice within the meaning of section 553(b)(A) of the APA. Therefore, publication in the *Federal Register* of a notice of proposed rulemaking and request for comments is not required. Furthermore, because this rule is procedural rather than substantive, the normal requirement of 5 U.S.C. 553(d) that a rule not be effective until at least 30 days after publication in the *Federal Register* is inapplicable. OSHA also finds good cause to provide an immediate effective date for this rule, because it imposes no obligations on parties outside the federal government and therefore no advance notice is required to enable employers or other private parties to come into compliance.

II. Legal Authority

The Occupational Safety and Health Act of 1970, 29 U.S.C. 651 et seq. (OSH Act) authorizes the Secretary to issue two types of occupational safety and health rules: standards and regulations. Standards, which are authorized by section 6 of the Act, specify remedial measures to be taken to prevent and control employee exposure to identified occupational safety and health hazards, while regulations are the means to effectuate other statutory purposes, including the maintaining of records. For example, the OSHA requirements at 29 CFR 1910.95 are a "standard" because they include remedial measures to address the specific and already identified hazard of employee exposure to occupational noise. In contrast, a "regulation" is a purely administrative effort designed to uncover violations of the Act and discover unknown dangers. The procedural regulations in 29 CFR 1913.10 are necessary to enable the use of employee medical records by OSHA consistent with the employee's right of privacy.

In section 2(b) of the OSH Act, Congress declared the overriding purpose of the Act is "to assure so far as possible every working man and woman in the Nation safe and healthful working conditions." (29 U.S.C. 651.) Congress also explicitly declared that this must be accomplished, among other ways, "by providing an effective enforcement program . . ." (29 U.S.C. 651(b)(10)). For the Secretary of Labor to conduct an effective enforcement program, he or she must determine whether occupational safety and health hazards exist in the workplace. To that end, the OSH Act authorizes the Secretary to enter and inspect workplaces and to conduct reasonable investigations into working conditions.

Section 8(a) of the OSH Act authorizes OSHA to enter, inspect, and investigate places of employment, and section 8(b) permits OSHA to subpoena both witnesses and

evidence when conducting inspections and investigations. (29 U.S.C. 657(a) and (b)). As noted above, in some instances, it may be necessary for OSHA to examine personally identifiable employee medical information. Section 8 of the OSH Act recognizes OSHA's right of access to medical records, and records access is mandated by OSHA standards and regulations, including 29 CFR 1910.1020(e)(3) (access to employee exposure and medical records). OSHA relies on administrative subpoenas to compel production of medical records by employers and other record holders.

OSHA is issuing the final rule pursuant to authority expressly granted in section 8 of the OSH Act. Section 8(c)(1) requires each employer to "make, keep, preserve, and make available to the Secretary [of Labor] or the Secretary of Health and Human Services, such records regarding his activities relating to this Act as the Secretary, in cooperation with the Secretary of Health and Human Services, may prescribe by regulation as necessary or appropriate for the enforcement of this Act or for developing information regarding the causes and prevention of occupational accidents and illnesses" (29 U.S.C. 657(c)(1)). Employee medical records are included within the type of records addressed by this provision.

Section 8(g)(1) of the OSH Act provides that the Secretary and Secretary of Health and Human Services are authorized to compile, analyze, and publish, either in summary or detailed from, all records or information obtained under this section (29 U.S.C. 657(g)(1)). Section 8(g)(2) is the general rulemaking authority of the OSH Act and provides that the Secretary and the Secretary of Health and Human Services shall prescribe such rules and regulations as he may deem necessary to carry out their

responsibilities under this Act, including rules and regulations dealing with the inspection of an employer's establishment.

III. Summary and Explanation of the Final Rule

Section 1913.10(b) - Scope and application.

OSHA's regulation at 29 CFR 1913.10(b), Scope and application, defines the circumstances under which the procedural regulations in § 1913.10 will apply. Except as provided in paragraphs (b)(3) through (6), the policies and procedures in § 1913.10 apply to all requests by OSHA personnel to access personally identifiable employee medical information.

In general, 29 CFR 1913.10 requires OSHA personnel to obtain a MAO (previously "written access order," but referred to in this section as "MAO" as it is in the final rule) when accessing personally identifiable employee medical information. However, under certain circumstances, the regulation states that OSHA access may be accomplished without obtaining a MAO. For example, § 1913.10(d)(4)(i) provides that a MAO is not needed when an employee gives specific written consent for OSHA to access their medical records. Also, § 1913.10(b)(3) through (5) include several categories of records that are not subject to § 1913.10 and therefore may be accessed without obtaining a MAO. These categories of records include medical information that is not in personally identifiable form, injury and illness records required by 29 CFR part 1904, death certificates, employee exposure records, and medical information obtained in the course of litigation. In addition, previous § 1913.10(b)(6) provided that the policies and procedures in § 1913.10 do not apply when a written directive by the Assistant Secretary authorizes appropriately qualified personnel to conduct limited review of specific medical

information mandated by an OSHA standard or of specific biological monitoring test results. This final rule amends § 1913.10(b)(6) to state that the MRO is now responsible for issuing these written authorization directives.

OSHA Directive CPL 02-02-072, Rules of agency practice and procedure concerning OSHA access to employee medical records, August 22, 2007, includes authorization for review of three categories of information based on the provisions in § 1913.10(b)(6). The directive authorizes OSHA compliance personnel to review (1) medical opinions mandated by OSHA standards, (2) information required by a medical surveillance program, and (3) certain information used to verify compliance with the injury and illness recordkeeping requirements in 29 CFR part 1904. OSHA personnel do not need a MAO when they access the information at a workplace pursuant to a written directive under § 1913.10(b)(6). Instead, OSHA personnel follow the procedures set forth in the written directive. The 2007 directive includes provisions on how OSHA personnel may access the specific types of information and how the information should be protected once in the agency's possession.

OSHA believes the MRO is in the best position to make determinations regarding written authorization under § 1913.10(b)(6). Section 1913.10(c)(2) already provides that the MRO must have experience or training in the evaluation, use, and privacy protection of medical records, and, as discussed below in this preamble, paragraph (c) of § 1913.10 has been amended to provide that the MRO is now responsible for the overall administration of the policies and procedures in § 1913.10. Also, as part of the final rule, paragraph (c) now states that the MRO is specifically responsible for making determinations regarding the approval of MAOs, inter-agency transfer, and public

disclosure of identifiable employee medical records. Given all the new MRO responsibilities set forth in paragraph (c), as well as the existing duties in the other paragraphs of the regulation, it is appropriate to also make the MRO responsible for written authorization under paragraph (b)(6). Accordingly, final § 1913.10(b)(6) states that the provisions of 29 CFR 1913.10 do not apply where a written directive by the MRO authorizes appropriately qualified personnel to conduct limited review of specific medical information mandated by an occupational safety and health standard or of specific biological monitoring test results. OSHA will also amend Directive CPL 02-02-072 to reflect the new regulatory text in paragraph (b)(6).

Section 1913.10(c) – Responsible persons.

OSHA's regulation at 29 CFR 1913.10(c) establishes certain responsibilities for OSHA personnel when the agency accesses personally identifiable employee medical information. Paragraph (c) is largely a summary of duties established by other paragraphs in § 1913.10 and sets forth specific responsibilities for the Assistant Secretary, MRO, and Principal OSHA Investigator. The final rule amends several provisions in paragraph (c) to emphasize the responsibilities of the MRO.

Under the previous regulation, paragraph (c)(1) provided that the OSHA Assistant Secretary was responsible for the overall administration and implementation of the policies and procedures in § 1913.10. This responsibility included making determinations regarding (1) OSHA access to personally identifiable employee medical information and (2) interagency transfer or public disclosure of personally identifiable employee medical information. Also under the previous regulation, § 1913.10(d)(1) provided that each request by an OSHA representative to access information through a

written access order must be approved by the Assistant Secretary upon the recommendation of the MRO.

Section 1913.10(c)(2) of the previous regulation provided that the Assistant Secretary was responsible for designating an OSHA official with experience or training in the evaluation, use, and privacy protection of medical records to be the MRO. The MRO, who reported directly to the Assistant Secretary on matters related to § 1913.10, was responsible for making recommendations to the Assistant Secretary on whether to approve or deny written access orders, and served as the central reviewer of the sufficiency and justification of these documents. The MRO was also responsible for responding to employee, collective bargaining agent, and employer objections to written access orders. In addition, § 1913.10(c)(2) of the previous regulation stated that the MRO was responsible for controlling the use of direct personal identifiers; controlling internal agency use and security of personally identifiable employee medical information; assuring that the results of agency analysis of personally identifiable employee medical information are, where appropriate, communicated to employees; preparing an annual report for the Assistant Secretary on OSHA's experience with respect to § 1913.10; and assuring that adequate notice is given of intended inter-agency transfers or public disclosures of personally identifiable employee medical information.

The other OSHA official with important responsibilities when the agency accesses employee medical information is the Principal OSHA Investigator. Section 1913.10(c)(3) provides that the Principal OSHA Investigator is the OSHA employee designated on the MAO who is primarily responsible for ensuring that OSHA examination and use of employee medical information is in accordance with the

provisions of the MAO and § 1913.10. In most instances, the Principal OSHA Investigator named on a MAO is an employee from an OSHA Regional or Area Office and determines how and when employee medical information will be accessed during an OSHA inspection or investigation. In practice, the Principal OSHA Investigator is responsible for ensuring that the provisions of the MAO and § 1913.10 are followed by OSHA personnel when medical information is accessed at a specific workplace. As provided in § 1913.10(c)(3), the Principal OSHA Investigator must be professionally trained in medicine, public health, or similar fields (epidemiology, toxicology, industrial hygiene, biostatistics, environmental health) when access is made pursuant to a MAO. The provisions in § 1913.10(c)(3) concerning the Principal OSHA Investigator are unchanged by the final rule.

The final rule retains the Assistant Secretary's responsibility to designate an OSHA official as MRO. However, this responsibility is now set forth in § 1913.10(c)(1). Like the previous regulation, § 1913.10(c)(1) of the final rule states that the Assistant Secretary shall designate an OSHA official with experience or training in the evaluation, use, and privacy protection of medical records to be the OSHA Medical Records Officer. The final rule also states that the Assistant Secretary may change the designation of the MRO at will.

The final rule includes several changes to paragraph (c)(2), OSHA Medical Records Officer. Some of these changes transfer specific responsibilities from the Assistant Secretary to the MRO while other responsibilities assigned to the MRO in § 1913.10(c)(2) are carried over from the previous regulation.

The final rule amends paragraph (c)(2) to provide that the MRO is now responsible for the overall administration and implementation of the procedures contained in § 1913.10. OSHA believes there are two central principles that form the basis of the procedural requirements in § 1913.10: (1) there should be a thorough review of all efforts to examine or copy personally identifiable employee medical information before the information is obtained and (2) personally identifiable information must be carefully protected once obtained. OSHA also believes the MRO is in the best position to ensure that the central principles of § 1913.10 are carried out by the agency.

As already noted, paragraph (c)(1) of the final rule, like the previous regulation, provides that the MRO must have experience and training in the evaluation, use, and privacy protection of medical records. Historically, a physician from OSHA's Office of Occupational Medicine and Nursing (OOMN) has been designated as MRO, and, in most cases, the person designated has been the Director of OOMN. As a result, the MRO has had an extensive background in both medicine and administration.

Additionally, under the previous regulation, the MRO was already responsible for ensuring the sufficiency and justification of MAOs and making recommendations to the Assistant Secretary on whether to approve or deny such documents. The MRO also has several duties set forth throughout the other paragraphs in § 1913.10 and therefore has a good understanding of the day-to-day implementation of the regulation.

Under the final rule, the MRO will now be responsible for making determinations regarding whether to approve or deny MAOs, any inter-agency transfer, and public disclosures of personally identifiable employee medical information, as well as whether to issue written directives authorizing OSHA personnel to conduct limited review of

certain medical information without an MAO. Accordingly, the extensive medical and administrative experience, the responsibilities under the previous regulation, and the new responsibilities assigned by this final rule make the MRO the logical OSHA official to have responsibility for the overall administration and implementation of the procedures in § 1913.10.

While the final rule limits the role of the Assistant Secretary in the day-to-day implementation of § 1913.10, the Assistant Secretary still maintains an important oversight responsibility. As in the previous regulation, the Assistant Secretary retains the responsibility for naming an OSHA official as MRO, with the ability to replace the MRO at will, and the MRO must still report to the Assistant Secretary on matters related to § 1913.10. In practice, the MRO will continue to consult with the Assistant Secretary on MAO approval, inter-agency transfers, and public disclosures of personally identifiable employee medical information. In addition, paragraph (l) requires the MRO to prepare an annual report for the Assistant Secretary on matters related to the approval and purpose of MAOs, objections to MAOs, and inter-agency transfers and public disclosures during the previous year. The responsibility to designate an OSHA official as MRO, continued consultation, and receiving reports from the MRO will keep the Assistant Secretary informed about OSHA's overall implementation of § 1913.10. Accordingly, like the previous regulation, the final rule at paragraph (c)(2) provides that the MRO is responsible for reporting directly to the Assistant Secretary on matters concerning § 1913.10.

Under the final rule, the MRO is also now responsible for making determinations concerning (1) access to personally identifiable employee medical information and

(2) interagency transfer or public disclosure of personally identifiable employee medical information. These two responsibilities had been assigned to the Assistant Secretary in previous § 1913.10(c)(1).

Section 1913.10(c)(2)(i) of the final rule states that the MRO is responsible for making determinations concerning OSHA access to personally identifiable employee medical information under § 1913.10(d). Paragraph (d) addresses OSHA access to personally identifiable employee medical information by MAO.

With the exception of two circumstances described at the end of paragraph (d), each request by OSHA to examine or copy personally identifiable employee medical information is made pursuant to an MAO. Paragraph (d)(2) sets criteria the agency must follow when it seeks access to identifiable medical information, and paragraph (d)(3) sets forth the content to be included in the MAO. In order to be valid, an MAO must be approved by the MRO using the criteria in paragraph (d)(2). First, the MRO must consider whether the information to be examined or copied is relevant to a statutory purpose and whether there is a need to gain access to the information. The MRO has the responsibility, on a case-by-case basis, to ensure that access is sought only where there is a genuine need to do so. OSHA believes that a finding of relevance and need by the MRO is a significant safeguard against excessive use of the agency's authority to access personally identifiable employee medical information.

Paragraph (d)(2) next states that consideration must be given to whether the personally identifiable employee medical information subject to the MAO is limited to only that information needed to accomplish the purpose for access. This provision is aimed at preventing OSHA access to extraneous medical information unrelated to the

purpose for access. Lastly, paragraph (d)(2) states that the MRO must determine that the personnel authorized to review the medical information are limited to those who have a need for access and have appropriate professional qualifications. The limiting of personnel that can review and analyze information to only those who have a need for access and who have appropriate professional qualifications is important for maintaining the confidentiality of employee medical records.

OSHA believes the MRO is in the best position to evaluate the criteria in paragraph (d) and make determinations on whether to approve or deny MAOs. Typically, the MRO has extensive subject-matter clinical experience and expertise in occupational medicine. This allows the MRO to evaluate whether, and to what extent, employee medical information needs to be accessed by OSHA. Accordingly, paragraph (d)(2) has been amended to state that, before approving an MAO, the MRO must determine that the documents meet the criteria in that paragraph.

For similar reasons, the MRO is also now responsible for making determinations concerning inter-agency transfer and public disclosure of personally identifiable employee medical information. Section 1913.10(m) describes the circumstances under which personally identifiable employee medical information can be transferred to another agency or disclosed to the public. The requirements in paragraph (m) remain unchanged from the previous regulation. However, the provisions in paragraph (m), as well as paragraph (c)(2), are amended by the final rule to provide that the MRO, not the Assistant Secretary, is now responsible for making determinations regarding inter-agency transfer and public disclosure of personally identifiable employee medical information. The

individual provisions in paragraph (m) are amended to cross reference with the new MRO responsibility established in § 1913.10(c)(2)(vii).

The following discussion of the individual provisions in paragraph (m) clarifies the MRO's new responsibility for making determinations concerning inter-agency transfer and public disclosure set forth in § 1913.10(c)(2). The previous regulation at § 1913.10(m)(1) stated that personally identifiable employee medical information shall not be transferred to another agency or office outside of OSHA (other than the Office of the Solicitor of Labor) or disclosed to the public (other than to the affected employee or the original recordholder) except when required by law or when approved by the Assistant Secretary. The final rule amends paragraph (c)(2)(vii) to make clear that the MRO is now responsible for making these determinations. The final rule also amends paragraph (m) to provide that the MRO must follow specific criteria when making determinations concerning inter-agency transfer and public disclosure of personally identifiable employee medical information.

OSHA's longstanding position is that inter-agency transfer and public disclosure of personally identifiable employee medical information should be carefully considered, and paragraph (m) addresses these issues. Inter-agency transfer and public disclosure of personally identifiable employee medical information are not categorically prohibited by the regulation for two reasons. OSHA believes (1) it cannot legally make such a commitment and (2) situations arise where transfer or disclosure is appropriate. Under certain circumstances, as a matter of law, OSHA is compelled to transfer information to another agency or disclose it to a non-governmental individual. For example, OSHA might be required to provide the information in response to a lawful subpoena. In other

circumstances, disclosure may also be appropriate. For example, in order to resolve a public health problem, OSHA may need to transfer employee medical information to another federal or state agency. In such situations, the transfer of employee medical information may be critical in identifying an emerging health issue, compiling data on worker fatalities from specific exposure, or evaluating the effectiveness of workplace controls designed to prevent occupational illness at manufacturing facilities.

OSHA notes that inter-agency transfer and public disclosure of personally identifiable employee medical information is not a common occurrence. In the last five years, the agency has made only three inter-agency transfers of personally identifiable employee medical information to another federal or state agency. OSHA also notes that inter-agency transfer and public disclosure of employee medical information not in personally identifiable form is not subject to provisions in § 1913.10.

Paragraph (m) of § 1913.10 includes strict limitations on inter-agency sharing and public disclosure of employee medical information. Except when required by law, all inter-agency transfer or public disclosure of personally identifiable employee medical information must be approved by the MRO in accordance with the criteria in paragraph (m).

Paragraph (m)(2) states that, except as provided for in paragraph (m)(3), the MRO shall not approve a request for an inter-agency transfer, which has not been consented to by the affected employee, unless the request is by a public health agency. Under this provision, transfer of medical information is permitted only to a public health agency for a substantial public health purpose. The regulation goes on to state that the MRO can approve the transfer only if the public health agency (1) needs the information for

substantial public health purposes, (2) will not use the information to make individual determinations concerning affected employees which could be to their detriment, (3) has regulations or written established procedures providing protection for personally identifiable medical information substantially equivalent to § 1913.10, and (4) satisfies an exemption to the Privacy Act to the extent the Privacy Act applies to the requested information.

Because OSHA collects medical information only for a public health purpose, OSHA believes it is appropriate to restrict all subsequent discretionary transfers to those agencies with an equivalent public health purpose. The MRO must review each request for a transfer on a case-by-case basis by taking into account each of the listed criteria in paragraph (m)(2). Most importantly, in order to protect individual privacy, the MRO must be satisfied that the recipient agency's privacy protections are equivalent to OSHA's.

Paragraph (m)(3) contains two exceptions to the requirements of paragraph (m)(2). First, upon the approval of the MRO, personally identifiable employee medical information can be shared with the National Institute for Occupational Safety and Health (NIOSH). Like OSHA, NIOSH is a public health agency and its research activities complement OSHA's regulatory responsibilities. OSHA's ability to analyze employee medical records is often improved by gaining NIOSH assistance, and medical information collected by OSHA may have major research value for NIOSH. Also, because of its frequent use of medical information, and sensitivity to individual privacy, NIOSH has procedures in place that provide for the protection of personally identifiable medical information that are substantially equivalent to § 1913.10. As a result, employee

medical information may be transferred to NIOSH if approved by the MRO without further inquiry into the sufficiency of its programs for protecting medical records.

Paragraph (m)(3) also permits, upon the approval of the MRO, the inter-agency transfer of personally identifiable employee medical information to the U.S. Department of Justice when necessary with respect to a specific action under the OSH Act. For example, the Justice Department prosecutes criminal violations under the OSH Act, as well as civil penalty collection actions. The Justice Department also represents OSHA in Freedom of Information Act (FOIA) lawsuits. Personally identifiable employee medical information may be relevant in these legal actions, and OSHA must be able to share information in these circumstances.

Paragraphs (m)(4) and (5) address public disclosure of personally identifiable employee medical information which has not been consented to by the affected employee. Paragraph (m)(4) provides that the MRO shall not approve a request for public disclosure of employee medical information containing personal identifiers unless there are compelling circumstances affecting the health or safety of an individual. Also, paragraph (m)(5) states that the MRO shall not approve a request for public disclosure of employee medical information which contains information which could reasonably be used indirectly to identify specific employees when the disclosure would constitute a clearly unwarranted invasion of personal privacy. Finally, paragraph (m)(6) retains the provision from the previous regulation that, except as to inter-agency transfer to NIOSH or the Department of Justice, the MRO shall ensure that advance notice is provided to any collective bargaining agent representing affected employees and to the employer on each occasion OSHA intends to transfer personally identifiable employee medical information

to another agency or disclose it to a member of the public other than to an affected employee. When feasible, the MRO must take reasonable steps to assure that advance notice is provided to affected employees when the employees' medical information to be transferred or disclosed contains direct personal identifiers.

Finally, the final rule at § 1913.10(c)(2) retains several provisions from the previous regulation. Specifically, paragraph (c)(2)(iii) continues to provide that the MRO is responsible for responding to MAO objections, and paragraph (c)(2)(iv) continues to provide that the MRO is responsible for overseeing the internal use and security of personally identifiable employee medical information. Two other MRO responsibilities in paragraph (c)(2) have been retained from the previous regulation but have been renumbered under the final rule. Paragraph (c)(2)(v), formerly paragraph (c)(2)(vi), continues to provide that the MRO is responsible for assuring that the results of agency analyses of personally identifiable medical information are, where appropriate, communicated to employees. Paragraph (c)(2)(vi), formerly paragraph (c)(2)(vii), retains the provision that the MRO is responsible for preparing an annual report of OSHA's experience under § 1913.10.

Section 1913.10(d)(1) – Requirements for medical access orders.

OSHA's previous regulation at § 1913.10(d)(1) stated that, except as provided in paragraph (d)(4), each request by an OSHA representative to examine or copy personally identifiable employee medical information contained in a record held by an employer or other record holder shall be made pursuant to a written access order which has been approved by the Assistant Secretary upon the recommendation of the OSHA Medical

Records Officer. Paragraph (d)(1) went on to state that, if deemed appropriate, a written access order may constitute, or be accompanied by, an administrative subpoena.

As explained above, the MRO is now responsible for the approval or denial of MAOs, and paragraph (d)(1) has been revised to reflect this change. The final rule also amends paragraph (d)(1) to make clear that a MAO does not constitute an administrative subpoena.

An administrative subpoena is a written order issued by OSHA to require an employer, or any other person, to produce listed records, documents, testimony and/or other supporting evidence relevant to an inspection or investigation under the OSH Act. If the person served with a subpoena refuses to honor (or only partially honors) the order, the subpoena is subject to judicial review and enforcement by a U.S. District Court. OSHA Regional Administrators have authority to issue administrative subpoenas and are also authorized to delegate to Area Directors the authority to issue routine administrative subpoenas. OSHA's policies and procedures for issuing an administrative subpoena are set forth in OSHA Instruction ADM 01-00-002, August 19, 1991.

In contrast, a MAO is an authorization for specified OSHA personnel to examine or copy personally identifiable employee medical information contained in a record held by an employer or some other record holder. Since an MAO relates to internal OSHA procedures, it cannot be used to compel the production of records, nor be enforced in a U.S. District Court. Historically, OSHA has not treated an MAO as equivalent to an administrative subpoena. OSHA's longstanding practice has been to rely on an administrative subpoena to compel production of medical records by employers. See OSHA's August 22, 2007, Instruction CPL 02-02-072, *Rules of agency practice and*

procedure concerning OSHA access to employee medical records. MAOs set forth internal OSHA procedure for assuring appropriate confidentiality of medical records is observed by OSHA personnel. As a result, except when reasonably certain that the employer will grant access to employee medical information, OSHA personnel present an administrative subpoena to the employer concurrently with an MAO.

The final rule amends § 1913.10(d)(1) to state that except as provided in paragraph (d)(4), each request by an OSHA representative to examine or copy personally identifiable employee medical information contained in a record held by an employer or other recordholder shall be made pursuant to a written medical access order which has been approved by the OSHA Medical Records Officer. A medical access order does not constitute an administrative subpoena.

Section 1913.10(g) – Removal of direct personal identifiers.

OSHA's previous regulation at § 1913.10(g) provided that all direct personal identifiers (e.g., name, address, Social Security Number, payroll number) must be removed by OSHA personnel whenever employee medical information obtained pursuant to a written access order is taken off-site, unless otherwise directed by the MRO. The regulation also required the Principal OSHA Investigator to code the medical information and the list of direct personal identifiers with a unique identifying number for each employee and then hand deliver or mail the list of identifiers to the MRO. The MRO thereafter controlled the use and distribution of the list of coded identifiers to those with a need to know its contents. In addition, the numerical coded medical information was to be used and kept secured as though still in a directly identifiable form.

Paragraph (g) was originally promulgated by OSHA when the rules of agency practice and procedure were issued in 1980. At that time, electronic medical records did not exist, and the employee records that did exist were maintained almost entirely in paper form. Since 1980, the number of medical records maintained by employers and other record holders has substantially increased, and the majority of these records are now maintained in electronic form.

The final rule revises § 1913.10 by deleting the outdated procedures set forth in paragraph (g). OSHA is eliminating this internal requirement for several reasons. First, existing access and safeguarding requirements in § 1913.10 already address privacy concerns when OSHA takes medical information away from a workplace for off-site review. Specifically, paragraph (h) of § 1913.10 provides that only authorized personnel may examine or copy personally identifiable employee medical information. As explained below, OSHA experience is that this process can result in coding and re-coding errors in individual employee medical records. Likewise, it provides that, unless an exception applies, OSHA personnel and contractors are authorized to use information only for the purpose for which it was obtained. In addition, paragraph (h)(5) states that, whenever practicable, the examination of personally identifiable employee medical information shall be conducted on-site with a minimum of medical information taken off-site in a personally identifiable form.

Additionally, paragraph (i) of § 1913.10 includes security procedures for handling personally identifiable employee medical information. For example, paragraph (i)(1) provides that files containing personally identifiable employee medical information shall be segregated from other agency files and, when not in active use, must be kept in a

locked cabinet or vault. In practice, the locking requirement extends to when medical information is transported from the workplace, as OSHA personnel place records in a locked trunk during transport by automobile.

Second, paragraph (n) of this final rule establishes new requirements for the access and safeguarding of personally identifiable employee medical information in electronic form. As discussed more extensively below, paragraph (n) of the final rule provides that the Principal OSHA Investigator is responsible for preventing any careless, accidental, or unintentional disclosure of, modification to, or destruction of electronic medical records. Paragraph (n)(3) of the final rule provides that the transfer and/or duplication of medical records in electronic form must be kept to the minimum necessary to accomplish the purpose for which it was obtained. Also, paragraph (n)(4) states that electronic files containing personally identifiable employee medical information shall be downloaded only to a computer hard drive or laptop that is secured (e.g., password protected). Paragraph (n)(4) now includes the Government standards that address secure access to Government systems and the data they contain: Federal Information Processing Standards (FIPS) 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors"; and HSPD-12, "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12)."

In addition, paragraph (n)(5) provides that electronic files containing personally identifiable employee medical information must be encrypted before transferred to authorized individuals. OSHA believes the safeguards for electronic medical records established by this final rule, which are based on existing OSHA practices and policy, enhance privacy protection and reduces the need to remove direct personal identifiers

when OSHA personnel take personally identifiable employee medical information off-site.

OSHA's experience is that de-identification increases the risk of mislabeling or misidentifying employee medical records and places a burden on agency resources by requiring additional OSHA staff time to accurately conduct de-identification and copying of employee medical records. In some cases, depending on the number of employees at a specific facility, OSHA employees may spend several hours finding and removing each direct personal identifier within each affected employee's medical record. The deletion of paragraph (g) will reduce the amount of time and physical space needed by OSHA personnel at a worksite.

Finally, the deletion of de-identification procedures in paragraph (g) will simplify follow-up communication from authorized OSHA personnel with individual employees after evaluation of their medical information. For example, by not having to complete a potentially extensive de-identification process, critical medical information about an employee will be reviewed by an OSHA physician sooner, and this will allow the physician to conduct follow-up consultation with the employee in a timely manner. Also, because personally-identifiable information will remain in the medical records taken from a workplace for off-site review, it will make it easier for the OSHA physician to identify employees, compare associated records, and contact individual employees.

For all of the above reasons, OSHA has concluded that the removal of direct personal identifier requirements in paragraph (g) should be deleted.

Section 1913.10(n) – Medical records maintained in electronic form.

In many cases, employers and other record holders maintain personally identifiable employee medical information in electronic form. OSHA's regulation at 29 CFR 1910.1020 provides that a "record" includes any item, collection, or grouping of information regardless of the form or process by which it is maintained (e.g., paper, document, microfilm, X-ray film, or automated data processing). Medical records may also be maintained on media such as magnetic tape, computer disks, USB storage devices (e.g., thumb drives), and online computer storage. Historically, OSHA personnel have followed the requirements in 29 CFR 1913.10 when accessing personally identifiable employee medical information maintained in electronic form. However, the regulation did not include provisions that specifically addressed electronic medical records. The final rule establishes new internal policies and procedures in paragraph (n) to § 1913.10 that specifically address OSHA access, use, and safeguarding of personally identifiable employee medical information maintained in electronic form.

Since the rules of agency practice and procedure were first issued in 1980, medical professionals have increasingly relied on the use and storage of medical records in electronic form. These records tend to improve the quality of health care and have several practical advantages over paper records. For example, electronic medical records can be accessed by health care professionals at any time from any given location. Legible records can also lead to more accurate diagnosis, treatment, and drug prescription. Electronic medical records are cost-effective because they take up less storage space and can be stored indefinitely. However, because they are in electronic form, these records also present unique challenges to security, privacy, and data integrity.

OSHA believes the best way to protect the security and confidentiality of personally identifiable employee medical information in electronic form is to prevent unauthorized access to such information. Several effective administrative, technological, and physical measures can be taken to protect electronic medical information from unauthorized access, use, disclosure, disruption, modification, or destruction. These methods include establishing specific security roles and responsibilities for OSHA officials, technology safeguards such as encryption or firewalls to protect against electronic breaches, ID/password protection for devices and information systems, and the use of anti-virus and intrusion detection software. The establishment of new internal OSHA policies and procedures in paragraph (n) of this final rule will effectively protect the security, privacy, and data integrity of employee medical information in electronic form.

Section 1913.10(n)(1) of the final rule provides that, in general, when accessing and/or copying personally identifiable employee medical information in electronic form, OSHA personnel shall follow the requirements set forth in 29 CFR 1913.10. As noted above, OSHA personnel have historically followed the rules of agency practice and procedure in § 1913.10 when accessing employee medical information in electronic form, and many of the provisions in § 1913.10 are applicable regardless of the format used to maintain information. As a result, unless specifically addressed in paragraph (n), OSHA personnel should continue to follow the rules of agency practice and procedure in paragraphs (a) through (m) when accessing and safeguarding electronic employee medical information.

Section (n)(2) of the final rule includes responsibilities for the Principal OSHA Investigator when OSHA personnel access personally identifiable employee medical information in electronic form. Specifically, paragraph (n)(2) states that when personally identifiable employee medical information in electronic form is taken off-site, the Principal OSHA Investigator is primarily responsible for ensuring that such information is properly used and kept secured. This provision is based on the requirement in paragraph (h)(1) of § 1913.10, which provides that the Principal OSHA Investigator is responsible for ensuring that medical information is used and kept secured in accordance with § 1913.10. Other specific responsibilities assigned to the Principal OSHA Investigator in paragraph (n)(2) include preventing any accidental or unintentional disclosure of, modification to, or destruction of personally identifiable employee medical information in electronic form (paragraph (n)(2)(i)); controlling the flow of data into, through, and from agency computer operations (paragraph (n)(2)(ii)); and ensuring that distribution and review of medical information in electronic form is limited to only those OSHA personnel and contractors with a need for access (paragraph (n)(2)(iii)). The requirement in paragraph (n)(2)(iii) is derived from § 1913.10(d)(2)(iii), which provides that, before approving a MAO, the MRO must determine that personnel authorized to review and analyze personally identifiable employee medical information are limited to those who have a need for access and have appropriate qualifications.

As discussed above, the Principal OSHA Investigator is the OSHA employee in the field with primary responsibility for ensuring that the examination and use of employee medical information is in accordance with § 1913.10. As such, the Principal OSHA Investigator is responsible for ensuring that the provisions in paragraph (n) are

followed by OSHA personnel when electronic medical information is accessed from a specific workplace. For example, this would include ensuring that access to personally identifiable employee medical records in electronic form is limited to only authorized personnel with a need to review the information, ensuring that employee medical information is only downloaded to a secured device (e.g., password protected), and verifying that medical information is deleted or destroyed when no longer needed by the agency.

Section 1913.10(n)(3) of the final rule provides that the transfer and/or duplication of medical information in electronic form shall be kept to the minimum necessary to accomplish the purpose for which it was obtained. This provision is similar to paragraph (i)(3) of § 1913.10, which states that the photocopying or other duplication of personally identifiable employee medical information shall be kept to the minimum necessary to accomplish the purpose for which the information was obtained.

In some cases, personally identifiable employee medical information in electronic form needs to be transferred or duplicated to facilitate internal OSHA review. For example, in order to conduct a proper workplace inspection or investigation, it may be necessary for OSHA personnel to transfer employee medical records to another OSHA employee with expertise on a specific occupational health hazard. Paragraph (n)(3) of the final rule permits the transfer and duplication of electronic medical information but only to authorized individuals with a need to review the information. Transfer and duplication are also limited to the minimum necessary to accomplish the purpose for which it was obtained. An example of this limitation might include the review of a medical record to determine whether an employee has sustained a work-related injury or illness. In such

cases, review of a medical record would extend only to information about the employee's injury or illness. In this example, the transfer and/or duplication of electronic medical information unrelated to the injury or illness would not be permitted.

Additionally, OSHA believes the likelihood that medical information in electronic form will be lost, altered, or destroyed increases during transfer or duplication. The duplication of electronic medical information can also raise concern about data integrity. For example, the copying or deleting of employee medical information from one document to another raises concern about the accuracy of the information. Accordingly, personally identifiable electronic medical information should be transferred only to authorized individuals with a need to know the information and should be duplicated only to facilitate authorized internal agency review.

Consistent with existing OSHA policy, § 1913.10(n)(4) of the final rule states that electronic files containing personally identifiable employee medical information shall be downloaded only to a computer hard drive or laptop that is in accordance with Federal Information Processing Standard (FIPS) 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," and "Homeland Security Presidential Directive 12: Policy for Common Identification Standard for Federal Employees and Contractors (HSPD-12)." The use of secured technology when downloading medical records will help to ensure that information is (1) accessed only by authorized individuals with a need-to-know and (2) not modified or deleted.

In accordance with current OSHA and Federal Government policy, the use of password protection is easy to implement, cost-effective, and a reliable method for securing electronic information. By downloading employee medical information to a

secured hard drive or laptop, OSHA personnel will be able to ensure that only individuals that know the password can open a document and read its content. This practice also provides a level of protection that goes with the document no matter where it is stored or sent. Finally, because tampering with a secured device takes time and effort, providing this level of protection acts as a deterrent to accessing document content by unauthorized individuals.

Additionally, it is important for OSHA personnel to follow proper security practices when using password protected devices containing personally identifiable employee medical information. Authorized individuals must not share their ID with others, should log-off when leaving a terminal, and use their own ID to access employee medical records. Also, authorized individuals should not keep written facsimiles of passwords or access codes. Other security measures, such as the use of firewalls, anti-virus software, and intrusion detection software should also be used to protect data integrity. Again, the Principal OSHA Investigator is responsible for ensuring that proper security measures are in place in the field to protect the confidentiality of personally identifiable employee medical records in electronic form.

Moreover, it is critically important that mobile devices be encrypted or use password protection when used to download, transfer, or store electronic medical information. Mobile devices are for individual use, and are not designed for centralized IT management. These devices can easily be manipulated, damaged, or stolen. By encryption, OSHA means the process of changing plain text into cypher text for the purpose of security. The use of encryption results in the encoding of information in such a way so that only authorized individuals can access the information.

Section 1913.10(n)(5) of the final rule states that electronic files containing personally identifiable employee medical information shall not be transferred to authorized personnel through email attachment unless appropriately encrypted. The transfer of employee medical information by email attachment increases the risk that such information will be sent to an unauthorized individual. The transfer of personally identifiable employee medical information in electronic form must be made through secured means. See §1913.10(n)(4), discussed above ("Electronic files containing personally identifiable employee medical information shall only be downloaded to a computer hard drive or laptop that is secured."). Appropriate methods for the transfer of personally identifiable employee medical information in electronic form may include the use of password protected or encrypted files on a secured agency website designed for confidential information, the mailing of encrypted computer disks or USB drives, the emailing of password protected medical records (Adobe secured), and the printing and hand delivery of paper records.

Paragraph (n)(6) provides that when an employer or other record holder(s) provides access to employee medical information through a properly encrypted email attachment, the attachment shall be downloaded to a secured hard drive or laptop. After the attachment is downloaded, the email shall be permanently deleted.

In some cases, employers and other record holders provide OSHA with access to employee medical information through an encrypted email attachment. As noted above, the use of email attachments to transfer medical records makes it more likely that the information will be sent to unauthorized individuals. Paragraph (n)(6) ensures that

medical information received in an encrypted email attachment is downloaded to a secured device.

After downloading the attachment from the employer or other record holder, the email must be permanently deleted to prevent transfer to unauthorized individuals. By permanently deleted, OSHA means that the email should be deleted so that it cannot be retrieved. Some email programs automatically delete trashed emails after a certain amount of time. Other programs retain emails until the user runs out of space. However, the intent of this provision is that, once the attachment is downloaded, OSHA personnel should immediately and permanently delete the incoming email. Most email programs have a "delete forever" function that allows the user to select emails in the trash folder for permanent deletion.

Section 1913.10(n)(7) of the final rule states that personally identifiable employee medical information in electronic form shall be secured when not in use. This provision is based on paragraph (i)(1) of § 1913.10, which states that agency files containing personally identifiable employee medical information shall be segregated from other agency files, and when not in active use, files containing this information shall be kept secured in a locked cabinet or vault. Paragraph (n)(7) is intended to prevent unauthorized access or modification to employee medical information in electronic form. In addition to all of the procedures in paragraph (n) addressing the use of electronic information by OSHA personnel, when not in use, such information must be stored in a secured manner. For example, when not in use, personally identifiable employee medical information should be stored on a password protected hard drive or laptop. Another example might be the storing of information on a password protected agency website designed to store

confidential information. Also, if employee medical records are kept on computer disk or other electronic storage media, when not in use, the disk or media should be stored under lock and key. Paragraph (n)(7)(i) of the final rule also emphasizes the importance of proper storage by specifically stating that medical information in electronic form shall only be maintained or stored where facilities and conditions are designed to prevent unauthorized access.

Paragraph (n)(7)(ii) provides that personally identifiable employee medical information in electronic form shall be maintained only for so long as needed to accomplish the purpose for access. This provision is derived from paragraph (j)(1) of § 1913.10, which provides that consistent with OSHA records disposition programs, personally identifiable employee medical information shall be destroyed or returned to the original record holder when no longer needed for the purposes for which they were obtained. In OSHA's view, maintaining medical records only for so long as needed helps to ensure that such information will not be accessed by unauthorized individuals.

In some cases, after its initial use by the agency, personally identifiable employee medical information may not be used again until sometime in the future. For example, medical information used as the basis for an OSHA citation may be used during the hearing stage of an enforcement case before the Occupational Safety and Health Review Commission. The medical information may not be used while the case is on appeal, but there may be a need for the information if the case is remanded for further judicial proceedings. Similarly, an investigation of an apparently new health hazard may produce uncertain results. Before completely closing out this investigation, it may be appropriate to await the outcome of an ongoing research study or parallel investigation elsewhere in

the country. In these cases, § 1913.10(j) provides that the medical information should be transferred to the MRO. Also, under § 1913.10(l)(2), the MRO must conduct an annual review of all centrally-held information to determine which information is no longer needed for the purposes for which it was obtained. These requirements apply equally to personally identifiable employee medical information stored in electronic form.

Paragraph (n)(7)(iii) of the final rules states that when no longer needed, the Principal OSHA Investigator shall ensure that all personally identifiable employee medical information on electric files has been deleted, destroyed, or returned to the original record holder. The requirement in paragraph (n)(7)(iii) is intended to ensure that the Principal OSHA Investigator is responsible for OSHA access and use of electronic medical information from beginning to end. When no longer needed, the Principal OSHA Investigator must make sure that authorized OSHA personnel follow proper procedures for the deletion, destruction and disposal of personally identifiable employee medical information. In practice, the Principal OSHA Investigator must ensure that media containing employee medical information is sanitized or destroyed before disposal or release for reuse in accordance with approved methods. In addition, if electronic medical records are returned to the original record holder, the Principal OSHA Investigator must ensure that all data is returned, and no data remains in the possession of OSHA personnel.

Paragraph (n)(7)(iv) states that the disposal of personally identifiable employee medical information maintained in electronic form shall be accomplished in such a manner as to make the data unattainable by unauthorized personnel. When no longer needed, electronic media must be handled and sanitized appropriately to prevent

unauthorized disclosure or modification of personally identifiable employee medical information.

OSHA personnel use several types of electronic media to access, use, and maintain personally identifiable employee medical information, including hard drives, laptops, USB storage drives (e.g., thumb drives), CDs, DVDs, and digital storage cards such as camera cards. In order to meet the requirement in paragraph (n)(7)(iv), and depending on the type of electronic media used, OSHA personnel may need to re-use, recycle, or destroy the electronic media containing medical information. Also, when employee medical information in electronic form is no longer needed, it is important to ensure that deleted data is not easily recoverable. Residual data may allow unauthorized individuals to reconstruct data and thereby gain access to personally identifiable employee medical information. Sanitization is one method that can be used to ensure that deleted data cannot be reconstructed.

Sanitization is the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed. There are different types of sanitization for each type of media, including cleaning, purging, and destroying. Cleaning is the removal of data from devices in such a way that there is assurance that the data cannot be reconstructed using normal system functions or software file/data recovery utilities. For example, cleaning may include using software or hardware products to overwhelm media with non-sensitive data. Purging is generally done before releasing media beyond control, such as before discarding old media, and includes degaussing or exposing media to a strong magnetic field in order to disrupt recorded magnetic domains. Destruction of media is the ultimate form of sanitization.

In some cases, OSHA personnel maintain employee medical information on media that may not be able to be reused such as computer disks and camera cards. In these situations, when no longer needed, electronic media containing personally identifiable employee medical information should be disposed of using approved secure data destruction. Several methods exist to dispose of electronic media containing medical information. For example, computer disks can be rendered unusable by shredding, incinerating, or pulverizing. Many OSHA Regional and Area Offices already have equipment that can shred or burn disks. Other offices contract with private companies to perform this task in a secure manner. As a reminder, in order to address security and privacy concerns, disposal operations should be conducted in accordance with approved DOL or OSHA methods. In addition, OSHA is responsible for the management of records pursuant to the Federal Records Act of 1950, as amended (44 U.S.C. Chapters 21, 29, 31, 33). The retention and destruction of Federal records must be conducted in accordance with the procedures described in the Federal Records Act.

Finally, in the future, OSHA personnel will be using media types not specifically mentioned in this preamble. The processes mentioned in this document should guide media sanitization and disposal decisions regardless of the type of media in use. In the future, OSHA will issue guidance to agency staff as new technology is developed.

IV. State Plans

The 28 states and U.S. territories with their own OSHA-approved occupational safety and health plans are encouraged, but not required, to adopt these rules of agency practice and procedure concerning employee medical record access that Federal OSHA is promulgating to 29 CFR 1913.10 in this final rule. The states and U.S. territories with

OSHA-approved occupational safety and health plans covering private employees and state and local government employees are Alaska, Arizona, California, Hawaii, Indiana, Iowa, Kentucky, Maryland, Michigan, Minnesota, Nevada, New Mexico, North Carolina, Oregon, Puerto Rico, South Carolina, Tennessee, Utah, Vermont, Virginia, Washington, and Wyoming. In addition, six states and U.S. territories have OSHA-approved state Plans that apply to state and local government employees only: Connecticut, Illinois, Maine, New Jersey, New York, and the Virgin Islands.

This final rule describes a Federal program change for which State Plan adoption is not required. However, State Plans are required to have standards, and an enforcement program, that are "at least as effective in providing safe and healthful employment" as those of Federal OSHA. In order to be "at least as effective" as Federal OSHA, a State Plan must appropriately utilize its authority for access to medical records, and must have effective procedures to assure that the privacy of those records is protected in a manner consistent with applicable state and federal privacy laws. Therefore, although adoption of this rule is not required, State Plans must have procedures covering this issue that are at least as effective as those of Federal OSHA and are encouraged to adopt requirements comparable to those in 29 CFR 1913.10.

Within 60 days of the effective date of this final rule, a State Plan must submit a notice of intent indicating whether they already have a similar policy in place, intend to adopt new policies and procedures, or do not intend to adopt this final rule. If a State Plan does not adopt at first, but at some later point decides to adopt this final rule or an at least as effective version of this final rule, the State Plan must notify OSHA of this change in intent. Within 60 days of adoption, the State Plan must provide an electronic

copy of the regulation or policy, or a link to where their policy is posted on the State Plan's website. The State Plan must also provide the date of adoption and identify differences, if any, between their policy and this final rule. OSHA will provide summary information on the State Plan responses to this instruction on its website at: *www.osha.gov/dcsp/osp/index.html*.

V. Regulatory Flexibility Certification

The notice and comment procedures of section 553 of the APA do not apply "to interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice." 5 U.S.C. 553(b)(A). Rules that are exempt from APA notice and comment requirements are also exempt from the Regulatory Flexibility Act (RFA). See SBA Office of Advocacy, A Guide for Government Agencies: How to Comply with the Regulatory Flexibility Act (August 2017); also found at *http://www.sba.gov/sites/default/files/rfaguide5F05125F0.pdf*. This is a rule of agency procedure, practice, and interpretation within the meaning of that section; and therefore, is exempt from both the notice and comment rulemaking procedures of the APA and the requirements of the RFA.

VI. Environmental Impact Analysis

In accordance with the requirements of the National Environmental Policy Act (NEPA) (42 U.S.C. 4231 et seq.), Council on Environmental Quality NEPA regulations (40 CFR parts 1500 through 1518), and the Department of Labor NEPA regulations (29 CFR part 11), OSHA has determined that this final rule will not have a significant impact on the external environment.

VII. Federalism

OSHA reviewed this final rule in accordance with the most recent Executive order on federalism (Executive Order 13132, 64 FR 43255, August 10, 1999). This Executive order requires Federal agencies, to the extent possible, to refrain from limiting state policy options, consult with states prior to taking any action that would restrict state policy options, and take such actions only when clear constitutional authority exists and the problem is national in scope.

This rule does not have "federalism implications." The rule does not have "substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government" and therefore is not subject to Executive Order 13132 (Federalism).

VIII. Unfunded Mandates

The Department has concluded that this rule is not a "significant regulatory action" within the meaning of Executive Order 12866, reaffirmed by Executive Order 13563, because it is not likely to (1) have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or state, local, or Tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in Executive Order 12866. Therefore, no economic impact analysis under section 6(a)(3)(C) of Executive

Order 12866 has been prepared. For the same reason, and because no notice of proposed rulemaking was published, no statement is required under section 202 of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1532. In any event, this rulemaking is procedural and interpretive in nature and is thus not expected to have a significant economic impact.

IX. Consultation and Coordination with Indian Tribal Governments

OSHA reviewed this rule in accordance with Executive Order 13175 (65 FR 67249, November 6, 2000) and determined that it does not have "tribal implications" as defined in that order. The rule does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

X. Office of Management and Budget Review Under the Paperwork Reduction Act of 1995

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 et seq.) and OMB regulations (5 CFR part 1320) require agencies to obtain approval from OMB before conducting any collection of information. The PRA defines a "collection of information" as "the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public of facts or opinions by or for an agency regardless of form or format" (44 U.S.C. 3502(3)(A)). The PRA does not apply to this final rule because it amends existing internal agency procedures and does not impose any new recordkeeping or information collection requirements that require OMB approval.

Authority and Signature

This document was prepared under the direction of Loren Sweatt, Principal Deputy Assistant Secretary for Occupational Safety and Health. It is issued under Section 8 of the Occupational Safety and Health Act (29 U.S.C. 657), 5 U.S.C. 553, 5 U.S.C. 552a(e), 5 U.S.C. 301, and Secretary of Labor's Order No. 5-2012 (77 FR 3912).

Signed at Washington, DC on July 14, 2020.

_____

Loren Sweatt,
Principal Deputy Assistant Secretary of Labor for Occupational Safety and Health.

Final Rule

Part 1913 of title 29 of the Code of Federal Regulations is hereby amended as follows:

PART 1913 -- [AMENDED]

1. The authority citation for part 1913 is revised to read as follows:

Authority: 29 U.S.C. 657; 5 U.S.C. 553; 5 U.S.C. 301; Secretary of Labor's Order No. 8-76 (41 FR 25059), 5-2002 (67 FR 65008), or 1-2012 (77 FR 3912) as applicable.

2. Amend §1913.10 by:

a. Revising paragraphs (b)(6), (c)(1) and (2), and (d)(1) and (2);

b. Removing and reserving paragraph (g);

c. Revising paragraph (m); and

d. Adding paragraph (n).

The revisions and addition read as follows:

§1913.10 Rules of agency practice and procedure concerning OSHA access to employee medical records.

* * * * *

(b) * * *

(6) This section does not apply where a written directive by the OSHA Medical Records Officer authorizes appropriately qualified personnel to conduct limited reviews of specific medical information mandated by an occupational safety and health standard, or of specific biological monitoring test results.

* * * * *

(c) * * *

(1) *Assistant Secretary*. The Assistant Secretary of Labor for Occupational Safety and Health (Assistant Secretary) shall designate an OSHA official with experience or training in the evaluation, use, and privacy protection of medical records to be the OSHA Medical Records Officer. The Assistant Secretary may change the designation of the OSHA Medical Records Officer at will.

(2) *OSHA Medical Records Officer*. The OSHA Medical Records Officer shall be responsible for the overall administration and implementation of the procedures contained in this section. The OSHA Medical Records Officer shall report directly to the Assistant Secretary on matters concerning this section and be responsible for:

(i) Making final determinations concerning the approval or denial of medical access orders (paragraph (d) of this section);

(ii) Assuring that medical access orders meet the requirements of paragraphs (d)(2) and (3) of this section;

(iii) Responding to objections concerning medical access orders (paragraph (f) of this section);

(iv) Overseeing internal agency use and security of personally identifiable employee medical information (paragraphs (g) through (j) of this section);

(v) Assuring that the results of agency analyses of personally identifiable medical information are, where appropriate, communicated to employees (paragraph (k) of this section);

(vi) Preparing an annual report of OSHA's experience under this section (paragraph (l) of this section); and

(vii) Making final determinations concerning inter-agency transfer or public disclosure of personally identifiable employee medical information (paragraph (m) of this section).

The Medical Records Officer shall also assure that advance notice is given of intended inter-agency transfers or public disclosures.

* * * * *

(d) * * *

(1) *Requirement for medical access order*. Except as provided in paragraph (d)(4) of this section, each request by an OSHA representative to examine or copy personally identifiable employee medical information contained in a record held by an employer or other recordholder shall be made pursuant to a written medical access order which has been approved by the OSHA Medical Records Officer. A medical access order does not constitute an administrative subpoena.

(2) *Approval criteria for medical access order*. Before approving a medical access order, the OSHA Medical Records Officer shall determine that:

(i) The medical information to be examined or copied is relevant to a statutory purpose and there is a need to gain access to this personally identifiable information;

(ii) The personally identifiable medical information to be examined or copied is limited to only that information needed to accomplish the purpose for access; and

(iii) The personnel authorized to review and analyze the personally identifiable medical information are limited to those who have a need for access and have appropriate professional qualifications.

* * * * *

(m) *Inter-agency transfer and public disclosure.* (1) Personally identifiable employee medical information shall not be transferred to another agency or office outside of OSHA (other than to the Office of the Solicitor of Labor) or disclosed to the public (other than to the affected employee or the original recordholder) except when required by law or when approved by the OSHA Medical Records Officer.

(2) Except as provided in paragraph (m)(3) of this section, the OSHA Medical Records Officer shall not approve a request for an inter-agency transfer of personally identifiable employee medical information, which has not been consented to by the affected employees, unless the request is by a public health agency which:

(i) Needs the requested information in a personally identifiable form for a substantial public health purpose;

(ii) Will not use the requested information to make individual determinations concerning affected employees which could be to their detriment;

(iii) Has regulations or established written procedures providing protection for personally identifiable medical information substantially equivalent to that of this section; and

(iv) Satisfies an exemption to the Privacy Act to the extent that the Privacy Act applies to the requested information (see 5 U.S.C. 552a(b); 29 CFR 70a.3).

(3) Upon the approval of the OSHA Medical Records Officer, personally identifiable employee medical information may be transferred to:

(i) The National Institute for Occupational Safety and Health (NIOSH); and

(ii) The Department of Justice when necessary with respect to a specific action under the Occupational Safety and Health Act.

(4) The OSHA Medical Records Officer shall not approve a request for public disclosure of employee medical information containing direct personal identifiers unless there are compelling circumstances affecting the health or safety of an individual.

(5) The OSHA Medical Records Officer shall not approve a request for public disclosure of employee medical information which contains information which could reasonably be used indirectly to identify specific employees when the disclosure would constitute a clearly unwarranted invasion of personal privacy (see 5 U.S.C. 552(b)(6); 29 CFR 70.26).

(6) Except as to inter-agency transfers to NIOSH or the Department of Justice, the OSHA Medical Records Officer shall ensure that advance notice is provided to any collective bargaining agent representing affected employees and to the employer on each occasion that OSHA intends to either transfer personally identifiable employee medical information to another agency or disclose it to a member of the public other than to an affected employee. When feasible, the OSHA Medical Records Officer shall take reasonable steps to assure that advance notice is provided to affected employees when the employee medical information to be transferred or disclosed contains direct personal identifiers.

(n) *Medical records maintained in electronic form*. (1) In general, when accessing and/or copying personally identifiable employee medical information in electronic form, OSHA personnel shall follow all of the requirements set forth in this section.

(2) When personally identifiable employee medical information in electronic form is taken off-site, the Principal OSHA Investigator is primarily responsible for ensuring that such information is properly used and kept secured.

(i) The Principal OSHA Investigator is responsible for preventing any accidental or unintentional disclosure of, modification to, or destruction of personally identifiable employee medical information in electronic form.

(ii) The Principal OSHA Investigator is responsible for controlling the flow of data into, through, and from agency computer operations.

(iii) The Principal OSHA Investigator shall ensure the distribution and review of medical information in electronic form is limited to only those OSHA personnel and contractors with a need for access.

(3) The transfer and/or duplication of medical information in electronic form shall be kept to the minimum necessary to accomplish the purpose for which it was obtained.

(4) Electronic files containing personally identifiable employee medical information shall be downloaded only to a computer hard drive or laptop that is secured in accordance with Federal Information Processing Standard (FIPS) 201-2 “Personal Identity Verification (PIV) of Federal Employees and Contractors” and “Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12).”

(5) Electronic files containing personally identifiable employee medical information shall not be transferred to authorized personnel through email attachment unless appropriately encrypted.

(6) When an employer or other record holder(s) provides access to employee medical information through a properly encrypted email attachment, the attachment shall be downloaded to a secured hard drive or laptop. After the attachment is downloaded, the email shall be permanently deleted.

(7) Personally identifiable employee medical information in electronic form shall be secured when not in use.

(i) Medical information in electronic form shall only be maintained or stored where facilities and conditions are designed to prevent unauthorized access.

(ii) Personally identifiable employee medical information in electronic form shall be maintained only for so long as needed to accomplish the purpose for access.

(iii) When no longer needed, the Principal OSHA Investigator shall ensure that all personally identifiable employee medical information on electronic files has been deleted, destroyed, or returned to the original record holder.

(iv) The disposal of personally identifiable employee medical information maintained in electronic form shall be accomplished in such a manner as to make the data unattainable by unauthorized personnel.

[FR Doc. 2020-15562 Filed: 7/29/2020 8:45 am; Publication Date: 7/30/2020]