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

(a) *General policy.* OSHA access to employee medical records will in certain circumstances be important to the agency's performance of its statutory functions. Medical records, however, contain personal details concerning the lives of employees. Due to the substantial personal privacy interests involved, OSHA authority to gain access to personally identifiable employee medical information will be exercised only after the agency has made a careful determination of its need for this information, and only with appropriate safeguards to protect individual privacy. Once this information is obtained, OSHA examination and use of it will be limited to only that information needed to accomplish the purpose for access. Personally identifiable employee medical information will be retained by OSHA only for so long as needed to accomplish the purpose for access, will be kept secure while being used, and will not be disclosed to other agencies or members of the public except in narrowly defined circumstances. This section establishes procedures to implement these policies.

(b) *Scope and application.*

(1) Except as provided in paragraphs (b) (3) through (6) below, this section applies to all requests by OSHA personnel to obtain access to records in order to examine or copy personally identifiable employee medical information, whether or not pursuant to the access provisions of 29 CFR 1910.1020(e).

(2) For the purposes of this section, “personally identifiable employee medical information” means employee medical information accompanied by either direct identifiers (name, address, social security number, payroll number, etc.) or by information which could reasonably be used in the particular circumstances indirectly to identify specific employees (e.g., exact age, height, weight, race, sex, date of initial employment, job title, etc.).

(3) This section does not apply to OSHA access to, or the use of, aggregate employee medical information or medical records on individual employees which is not in a personally identifiable form. This section does not apply to records required by 29 CFR part 1904, to death certificates, or to employee exposure records, including biological monitoring records treated by 29 CFR 1910.1020(c)(5) or by specific occupational safety and health standards as exposure records.

(4) This section does not apply where OSHA compliance personnel conduct an examination of employee medical records solely to verify employer compliance with the medical surveillance recordkeeping requirements of an occupational safety and health standard, or with 29 CFR 1910.1020. An examination of this nature shall be conducted on-site and, if requested, shall be conducted under the observation of the recordholder. The OSHA compliance personnel shall not

record and take off-site any information from medical records other than documentation of the fact of compliance or non-compliance.

(5) This section does not apply to agency access to, or the use of, personally identifiable employee medical information obtained in the course of litigation.

(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.

(7) Even if not covered by the terms of this section, all medically related information reported in a personally identifiable form shall be handled with appropriate discretion and care befitting all information concerning specific employees. There may, for example, be personal privacy interests involved which militate against disclosure of this kind of information to the public (*See,* 29 CFR 70.26 and 70a.3).

(c) *Responsible persons —*

(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.

(3) *Principal OSHA Investigator.* The Principal OSHA Investigator shall be the OSHA employee in each instance of access to personally identifiable employee medical information who is made primarily responsible for assuring that the examination and use of this information is performed in the manner prescribed by a written access order and the requirements of this section (paragraphs (d) through (m). When access is pursuant to a written access order, the Principal OSHA Investigator shall be professionally trained in medicine, public health, or allied fields (epidemiology, toxicology, industrial hygiene, biostatistics, environmental health, etc.).

(d) *Written access orders —*

(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.

(3) *Content of written access order.* Each written access order shall state with reasonable particularity:

(i) The statutory purposes for which access is sought,

(ii) A general description of the kind of employee medical information that will be examined and why there is a need to examine personally identifiable information,

(iii) Whether medical information will be examined on-site, and what type of information will be copied and removed off-site,

(iv) The name, address, and phone number of the Principal OSHA Investigator and the names of any other authorized persons who are expected to review and analyze the medical information.

(v) The name, address, and phone number of the OSHA Medical Records Officer, and

(vi) The anticipated period of time during which OSHA expects to retain the employee medical information in a personally identifiable form.

(4) *Special situations.* Written access orders need not be obtained to examine or copy personally identifiable employee medical information under the following circumstances:

(i) *Specific written consent.* If the specific written consent of an employee is obtained pursuant to 29 CFR 1910.1020(e)(2)(ii), and the agency or an agency employee is listed on the authorization as the designated representative to receive the medical information, then a written access order need not be obtained. Whenever personally identifiable employee medical information is obtained through specific written consent and taken off-site, a Principal OSHA Investigator shall be promptly named to assure protection of the information, and the OSHA Medical Records Officer shall be notified of this person's identity. The personally identifiable medical information obtained shall thereafter be subject to the use and security requirements of paragraphs (h) through (m) of this section.

(ii) *Physician consultations.* A written access order need not be obtained where an OSHA staff or contract physician consults with an employer's physician concerning an occupational safety or health issue. In a situation of this nature, the OSHA physician may conduct on-site evaluation of employee medical records in consultation with the employer's physician, and may make necessary personal notes of his or her findings. No employee medical records, however, shall be taken off-site in the absence of a written access order or the specific written consent of an employee, and no notes of personally identifiable employee medical information made by the OSHA physician shall leave his or her control without the permission of the OSHA Medical Records Officer.

(e) *Presentation of written access order and notice to employees.*

(1) The Principal OSHA Investigator, or someone under his or her supervision, shall present at least two (2) copies each of the written access order and an accompanying cover letter to the employer prior to examining or obtaining medical information subject to a written access order. At least one copy of the written access order shall not identify specific employees by direct personal identifier. The accompanying cover letter shall summarize the requirements of this section and indicate that questions or objections concerning the written access order may be directed to the Principal OSHA Investigator or to the OSHA Medical Records Officer.

(2) The Principal OSHA Investigator shall promptly present a copy of the written access order (which does not identify specific employees by direct personal identifier) and its accompanying

cover letter to each collective bargaining agent representing employees whose medical records are subject to the written access order.

(3) The Principal OSHA Investigator shall indicate that the employer must promptly post a copy of the written access order which does not identify specific employees by direct personal identifier, as well as post its accompanying cover letter (*See*, 29 CFR 1910.1020(e)(3)(ii)).

(4) The Principal OSHA Investigator shall discuss with any collective bargaining agent and with the employer the appropriateness of individual notice to employees affected by the written access order. Where it is agreed that individual notice is appropriate, the Principal OSHA Investigator shall promptly provide to the employer an adequate number of copies of the written access order (which does not identify specific employees by direct personal identifier) and its accompanying cover letter to enable the employer either to individually notify each employee or to place a copy in each employee's medical file.

(f) *Objections concerning a written access order.* All employee, collective bargaining agent, and employer written objections concerning access to records pursuant to a written access order shall be transmitted to the OSHA Medical Records Officer. Unless the agency decides otherwise, access to the records shall proceed without delay notwithstanding the lodging of an objection. The OSHA Medical Records Officer shall respond in writing to each employee's and collective bargaining agent's written objection to OSHA access. Where appropriate, the OSHA Medical Records Officer may revoke a written access order and direct that any medical information obtained by it be returned to the original recordholder or destroyed. The Principal OSHA Investigator shall assure that such instructions by the OSHA Medical Records Officer are promptly implemented.

(g) [Reserved]

(h) *Internal agency use of personally identifiable employee medical information.*

(1) The Principal OSHA Investigator shall in each instance of access be primarily responsible for assuring that personally identifiable employee medical information is used and kept secured in accordance with this section.

(2) The Principal OSHA Investigator, the OSHA Medical Records Officer, the Assistant Secretary, and any other authorized person listed on a written access order may permit the examination or use of personally identifiable employee medical information by agency employees and contractors who have a need for access, and appropriate qualifications for the purpose for which they are using the information. No OSHA employee or contractor is authorized to examine or otherwise use personally identifiable employee medical information unless so permitted.

(3) Where a need exists, access to personally identifiable employee medical information may be provided to attorneys in the Office of the Solicitor of Labor, and to agency contractors who are

physicians or who have contractually agreed to abide by the requirements of this section and implementing agency directives and instructions.

(4) OSHA employees and contractors are only authorized to use personally identifiable employee medical information for the purposes for which it was obtained, unless the specific written consent of an employee is obtained as to a secondary purpose, or the procedures of paragraphs (d) through (g) of this section are repeated with respect to the secondary purpose.

(5) Whenever practicable, the examination of personally identifiable employee medical information shall be performed on-site with a minimum of medical information taken off-site in a personally identifiable form.

(i) *Security procedures.*

(1) Agency files containing personally identifiable employee medical information shall be segregated from other agency files. When not in active use, files containing this information shall be kept secured in a locked cabinet or vault.

(2) The OSHA Medical Records Officer and the Principal OSHA Investigator shall each maintain a log of uses and transfers of personally identifiable employee medical information and lists of coded direct personal identifiers, except as to necessary uses by staff under their direct personal supervision.

(3) The photocopying or other duplication of personally identifiable employee medical information shall be kept to the minimum necessary to accomplish the purposes for which the information was obtained.

(4) The protective measures established by this section apply to all worksheets, duplicate copies, or other agency documents containing personally identifiable employee medical information.

(5) Intra-agency transfers of personally identifiable employee medical information shall be by hand delivery, United States mail, or equally protective means. Inter-office mailing channels shall not be used.

(j) *Retention and destruction of records.*

(1) Consistent with OSHA records disposition programs, personally identifiable employee medical information and lists of coded direct personal identifiers shall be destroyed or returned to the original recordholder when no longer needed for the purposes for which they were obtained.

(2) Personally identifiable employee medical information which is currently not being used actively but may be needed for future use shall be transferred to the OSHA Medical Records Officer. The OSHA Medical Records Officer shall 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.

(k) *Results of an agency analysis using personally identifiable employee medical information.* The OSHA Medical Records Officer shall, as appropriate, assure that the results of an agency analysis using personally identifiable employee medical information are communicated to the employees whose personal medical information was used as a part of the analysis.

(l) *Annual report.* The OSHA Medical Records Officer shall on an annual basis review OSHA's experience under this section during the previous year, and prepare a report to the Assistant Secretary which shall be made available to the public. This report shall discuss:

(1) The number of written access orders approved and a summary of the purposes for access,

(2) The nature and disposition of employee, collective bargaining agent, and employer written objections concerning OSHA access to personally identifiable employee medical information, and

(3) The nature and disposition of requests for inter-agency transfer or public disclosure of personally identifiable employee medical information.

(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.

[45 FR 35294, May 23, 1980; 45 FR 54334, Aug. 15, 1980, as amended at 71 FR 16674, Apr. 3, 2006; 85 FR 45792, July 30, 2020]