Attachment 24 –
OCISO Standard for Limiting the Use of Social Security Numbers in CDC Information Systems

Attachment A. SSN Elimination or Usage Approval Request for NIOSH Miners' Health System (MHS)

Date Submitted: 2/2/2017

Submitted by: Janet Hale, Security Steward

Office/Branch: CDC/NIOSH/ Respiratory Health Division/Office of the Director

Telephone: (304) 285-6264

Select Recommended Path forward:

☐ **C**

A. Eliminate the use of SSNs within < System Name >. The milestone date for complete elimination of SSNs is: <Date>. A certification of completion must be provided to the appropriate ISSO on or before this date.

☑ **C**

B. Request the CDC Senior Official for Privacy (SOP), approve collecting, processing, or storing SSNs in **Miners Health System (MHS),** within the parameters stipulated in the *OCISO Standard for Limiting the Use of Social Security Numbers in CDC Information Systems*.

If Option A is selected, only Section 4 of this form must be completed. If Option B is selected, please complete all remaining sections of this form:

1. JUSTIFICATION. *Briefly describe the purpose of the system and the mission and/or business justification for using SSNs. Reference any mandates or policies supporting the justification (such as approvals under the OMB Information Collection Request [ICR] process), and attach a copy to this request.*

The Federal Coal Mine Health and Safety Act of 1969 (as amended by the Federal Mine Safety and Health Act of 1977) is intended to protect the health and safety of underground coal miners. This Act directs NIOSH to study the causes and consequences of coal-related respiratory disease and, in cooperation with the Mine Safety and Health Administration (MSHA), to carry out a program for early detection and prevention of coal workers' pneumoconiosis. These activities are administered through the Coal Worker's Health Surveillance Program (CWHSP), as specified in the Federal Regulations, 41 CFR 37, "Specifications for Medical Examinations of Underground Coal Miners." The data (from the past 40 years) is stored in the CDC NIOSH Miners Health System (MHS).

When miners have a chest radiograph taken at an approved NIOSH facility, they are required to complete a Miner ID Form (OMB #0920-0020), which includes the miner's SSN (Part 37.20).The miner is required to provide the last 4 digits of the SSN and voluntarily provides the full SSN. The partial SSN, name, and birth date are used to verify the miner's identity and group all of their radiographs together by a sequential Miner Identification Number. If a miner has changes consistent with pneumoconiosis or other conditions, then all of their radiographs are pulled for comparison of progression of that condition. If a miner has a question regarding their radiograph, they provide their partial SSN, name, and birth

date for us to locate their records. The name and birth date is not enough information to uniquely identify a miner and a partial SSN is needed to make sure we have grouped all of a miner's radiographs together. NIOSH would not be able to understand the progression of Coal Worker's Pneumoconiosis (CWP), and miners would not have the benefit of previous chest radiographs to better interpret findings.

B Reader certification is granted to physicians with a valid U.S. state medical license who demonstrate proficiency in the classification of chest radiographs for the pneumoconiosis using the International Labour Office (ILO) Classification System. Proficiency is evaluated via the B Reader Examination. When a physician takes the B Reader Examination, he/she completes the Reader Certification Document (OMB #0920-0020), which includes the physician's SSN (last four digits required). As part of the CWHSP, a physician records their classification on the X-Ray Reading Sheet (OMB #0920-0020) findings. In the past, we used the physician SSN to track their status and record which physician classified the x-ray Physician SSNs will be eliminated from the database by June 15, 2017. The number of physicians used in the system is much smaller than the number of miners and physicians have a National Physician Index and Medical License number that can be used to verify identity. Digital archived documents will still have the physician's SSN.

2. **BACKGROUND.** *Describe additional information necessary for effective decision-making.*

(1) ALTERNATIVES. Provide an explanation of alternatives considered to collecting, using or storing SSNs and why the alternatives will not meet CDC mission and/or business needs.

We have held discussions trying to determine if we could remove the miner SSN from the system and have not found a method that would work in keeping the radiographs associated with a miner. We need several fields of information to resolve mistakes and uniquely identity miners. Miner addresses change often and not all miners have a driver's license. Physician SSNs will be removed from the database by June 15, 2017.

(2) E-AUTHENTICATION. *Provide an explanation of how any externally-facing system will/does achieve EAuthentication Level 3 (as described in the Certification & Accreditation package or the Change Request).*

MHS uses 2 levels of E-Authentication.

Level 1 for write only data and form submissions. External users at hospitals and clinics collect data from miners and send to NIOSH using the CDC Secure Access Management Services (SAMS) File Upload Tool.

Level 3 for read/write radiograph submissions. External users at hospitals and clinics acquire a chest radiograph of miners and send to NIOSH using a SAMS protected web site (PICOM Web).

SAMS uses HTTPS for securing data in transit and MHS servers utilize whole disk encryption for data at rest.

(3) *DATA AT REST ENCRYPTION. Provide an explanation of how and when the system will employ technologies to use FIPS 140-2 validated encryption of key personally identifiable information (PII) data elements at rest, to include SSNs.*

The MHS System has several components where SSNs reside:

A. The DRDS_UCMS database located on the SQP-103 server. This server uses full encryption. No further action is needed for this database.

B. The DRDS_ARCHIVE database located on the SQP-103 server. This server uses full encryption. No further action is needed for this database.

C. The DRDS_ARCHIVE scanned image files located on the WIPV-UCMS-ARCH server. No further action is needed for these images.

D. The DRDS_SIMS_PATIENT database located on the DSPV-INFC-1101 server. This database has SQL Transparent Data Encryption enabled and no further action is needed for this database.

E. The radiographs stored on ASPV-SIMS1 and AIPZ-SIMS1 use whole disk encryption and no further action is needed for these images.

F. OMB approved forms are stored on ITSO MUST encrypted storage. No further action is needed for the forms.

(4) OTHER FACTS OR ASSUMPTIONS. *Describe any other factors that are relevant to the decision, whether true now ("fact") or reasonably expected be in the future ("assumption").*

3. IMPACT OF SUCCESS OR FAILURE. *State the results, in terms of business outcomes, of approving or not approving this request.*

If this plan is not approved, NIOSH will not be able to service the miners with chest radiograph comparisons showing progression of disease.

4. APPROVAL. *Business Steward Sign and Date only-*

[redacted]	**NAME**	**DATE**
Business Steward Signature	2/3/2017 X Anita L. Wolfe Anita L. Wolfe Public Health Advisor Signed by: Anita L. Wolfe -S	
Business Steward Printed Name	**Anita Wolfe**	[redacted]

<u>For SOP Only --Decision and Signature</u>:

Approved: _____ Disapproved: _____

X _____

Beverly E Walker
Chief Privacy Officer