

# **Personally Identifiable Information Disclosure of the collection, storage and sharing of OCME Personally Identifiable Information pursuant to 74 O.S. § (2019) 3106.4(C)**

## **I. Medicolegal Board of Investigation (OCME)**

### **A. OCME Human Resources**

i. OCME Human Resources department receives the following personally identifiable information (PII) from employees during the onboarding process:

- a. Name
- b. Birthdate
- c. Social Security Number
- d. Official state or government issued driver license or identification number
- e. Alien registration number
- f. Government passport number

ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. OCME Human Resources does not share the personally identifiable information with anyone outside of OCME with the exception of the Oklahoma Public Employees Retirement System/Pathfinder. OCME limits access to this information to OCME Human Resources personnel and will share such information with OCME Employee Benefits Department on an as needed basis.

- a. In the event an applicant submits a resume that includes personally identifiable information other than what is listed above, Human Resources receives that as well.

iv. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

v. The applications are shared with the supervisor posting the job.

### **B. OCME Employee Benefits Department (Human Resources)**

i. OCME Employee Benefits Department collects the following via the Newly Eligible Form for plan participation on newly hired state employees and their dependents:

- a. Name
- b. Social Security Number
- c. Birthdate
- d. Phone Numbers
- e. Mailing Address
- f. Email Address
- g. Employing Agency
- h. Date of Hire
- i. Salary

- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. The information on all state employees is shared with Employees Group Insurance Division.
  - a. The information on state employees enrolled in medical or daycare reimbursement accounts is shared with the contractor administering this service.
  - b. The name and social security number of state employees contributing to a health savings account is shared with the contractor administering this service.
- iv. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

## **II. Information Services**

- A. OCME PII is stored by OMES in a manner consistent with the State's security policy and applicable regulatory requirements.
  - i. OCME does not share PII with any public body unless subpoenaed for the information.

## **III. Employees Group Insurance**

### **A. Employees Group Insurance Division (EGID)**

- i. EGID stores the following personally identifiable information of its members.
  - a. Name
  - b. Date of birth
  - c. Home address
  - d. Email addresses
  - e. Office address
  - f. Personal phone number
  - g. Business phone number
  - h. Social security number
  - i. Employee ID number
  - j. Employer ID number
  - k. Employment information
  - l. Financial information
  - m. Medicare ID
  - n. Personal Health Information (PHI).
    - PHI includes the demographic information listed in items a. – m. above, plus insurance claims payment data for EGID's HealthChoice plans. This may include dates of service, provider names, diagnoses, payment amounts, and limited specific medical data necessary to determine appropriate healthcare payments for a specific claim under terms of the plan's benefits.
  - o. Tax ID numbers and National Provider Identifiers of healthcare providers, as well as items a., b., d., e., g., h., k., l. and m. listed above for those providers.

ii. The PII collected is stored by EGIB in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. With Whom Personally Identifiable Data is Being Shared

a. As a HIPAA covered entity EGID may not use or disclose PHI except as permitted or required by federal and state statutes or rules. Disclosure of PHI is only performed by trained personnel in accordance with applicable laws, regulations and policies and procedures.

b. EGID shares PHI with

1. Individual insureds
2. Individuals authorized by the insured
3. Business Associates (as defined by 45 CFR 160.103) performing functions and activities that require access to PHI
4. Healthcare providers furnishing services which require access to PHI.

c. PHI may be disclosed in the following situations without a member's authorization when certain requirements are satisfied in accordance with 45 CFR 164.512. OCME has procedures describing the specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the EGIB Privacy Officer or legal counsel. These disclosures are:

1. Regarding victims of abuse, neglect or domestic violence
2. For treatment purposes
3. For judicial and administrative proceedings
4. For law enforcement purposes.
5. For public health activities
6. Regarding an individual who has died
7. For cadaveric organ-, eye- or tissue-donation purposes
8. For certain limited research purposes
9. To avert a serious threat to health or safety
10. For specialized government functions
11. That relate to workers' compensation programs

d. EGID makes reasonable efforts to limit disclosures and requests for PHI to the minimum necessary information needed to accomplish the intended purpose of the disclosure or request. For recurring processes, EGID has developed procedures and protocols that limit disclosures to the reasonably minimum amount required. All other requests are reviewed on an individual basis to meet the minimum necessary requirement.

e. The minimum necessary rule is not required to be applied under the following circumstances:

1. For treatment
2. For disclosure to the involved member
3. In accordance with the member's valid authorization
4. To the Office of Civil Rights for HIPAA compliance purposes

5. As required by law

#### **IV. OCME Capital Assets Management (CAM)**

##### **A. Capitol Reservations**

i. For persons and organizations reserving areas of the Capitol for events, OCME collects information for OMES:

- a. full name
- b. address
- c. phone number
- d. email address

ii. The PII collected is stored by OCME/OMES in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. This information is generally not shared outside of OCME/OMES.

##### **B. Capital Planning**

i. For capital outlay requests, OCME collects:

- a. contact name
- b. contact phone number
- c. contact email address

ii. The PII collected is stored by OCME/OMES in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. This information may be shared with the Long-Range Capital Planning Commission.

##### **C. Construction and Properties**

i. For consultants and/or businesses seeking state contracts, OCME collects a principal contact's name

- b. title
- c. telephone number
- d. address
- e. FEI/Tax ID number for the business entity

ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. This information may be shared with the using agency (i.e., the agency for whom the construction is being done). Otherwise, this information is not shared outside of OCME/OMES.

##### **D. Real Estate and Leasing Services**

i. Landlords who lease real property to the State and individuals or businesses seeking easements across state-owned property are required to provide:

- a. the firm or individual's name
- b. address
- c. phone
- d. email address

e. Social Security Number or FEI Number

- ii. The PII collected is stored by OCME/OMES in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. This information may be shared with the state agency for whom the space is being leased.

**E. Facilities Services**

i. For individuals submitting a Tenant Work Request in a building managed by OCME/OMES, OCME collects:

- a. a contact name
- b. phone number
- c. email.

- ii. The PII collected is stored by OCME/OMES in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. This information is generally not shared outside of OCME/OMES.

**F. Central Printing and Interagency Mail**

i. Central Printing collects:

- a. full name
- b. business address
- c. business phone number
- d. business email address for individuals ordering business cards and/or stationery
- e. Central Printing also collects names and addresses when necessary for mailing labels.

- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. Information on mailing labels is shared with the United States Postal Service. Otherwise, the above information is not shared outside of OCME.

**G. RISK Management**

i. OCME/OMES collects the following information regarding individuals having a possible claim against the State:

- a. Name
- b. Address
- c. Phone
- d. email address
- e. description of injury
- f. name of treating doctor and/or hospital.

- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. This information may be shared with other state agencies (if the claim involves another agency's employees or property), insurance companies for the State and/or claimant, a third-party administrator, and the Attorney General's Office, which provides legal counsel for Risk Management.

#### **H. Fleet Management**

- i. For drivers using Fleet Management vehicles, OCME/OMES collects:
  - a. the driver's name
  - b. employee identification number
  - c. email
  - d. phone number
- ii. The PII collected is stored by OCME/OMES in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. This information is generally not shared outside of OCME/OMES.

#### **I. Capitol-Medical Center Improvement and Zoning Commission**

- i. For persons requesting rezoning, zoning variances, historic preservation review, building or sign permits, or conditional use permits, the Commission collects:
  - a. applicant's street address
  - b. phone number
  - c. and email
- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. This information is used by OCME staff support for the Commission and the Commission itself.

#### **J. Surplus Property**

- i. Applicants for the Federal Property Donation Program are asked to provide:
  - a. Address
  - b. phone number
  - c. email address
  - d. federal ID number
- ii. Persons bidding online on state surplus property are required to provide:
  - a. Name
  - b. Address
  - c. phone number
  - d. email address
  - e. a credit or debit card
- iii. Persons bidding at the live monthly public auction may provide:
  - a. credit or debit cards, or check.
  - b. For persons paying with check, OCME also collects their driver's license number.
- iv. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iv. This information is generally not shared outside of OCME.

#### **V. Central Accounting and Reporting**

**A. Transaction Processing - Payroll Processing**

- i. Payroll Processing collects the following PII to generate payroll payments for the state:
  - a. Name
  - b. Employee ID
  - c. Pay amount (gross-net)
- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. The PII is not shared with anyone outside of OCME.

**B. Transaction Processing - Voucher Processing**

- i. Voucher Processing collects the following PII to process payments in People Soft:
  - a. Payee/Vendor/Supplier Name
  - b. Payee/Vendor/Supplier PeopleSoft ID
  - c. Business addresses (occasionally home address such as a board member payment).
- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. The Acct pay department does not share the PII information with anyone outside of OCME

**C. Transaction Processing - Replacement Warrant Processing**

- i. Collects the following PII by OCME Acct pay and used for processing replacement payments of statutory cancelled warrants and lost or destroyed warrants:
  - a. Payee/Vendor/Supplier Name
  - b. Payee/Vendor/Supplier PeopleSoft ID
- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. The PII is not shared with anyone outside of OCME or others with proper access.

**D. Payroll**

- i. Payroll collects the following PII from OCME HR/Payroll and other agencies to generate payroll and provide W-2's and required reporting to applicable state and federal government entities:
  - a. Name
  - b. Birthdate
  - c. Social Security Number
  - d. Medical Information
  - e. Employment Information
- ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.
- iii. The payroll department does not share the PII with anyone outside of OCME, or the specific shared service agency, with the exception of OPERS, OLERS, DHS, Oklahoma and other state's tax commissions, Oklahoma and other state's employment commission, the Social Security Administration and the IRS.

### **E. Vendor Registration**

i. Vendor Registration collects the following PII from OCME Vendor Payee Form, OCME Employee Form, OCME Garnishment Vendor Request Form, and OCME Disregarded Entity Questionnaire:

- a. Name
- b. Taxpayer ID Number
- c. Bank Account Information

ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

iii. Financial registration access, information and documentation is protected information. A secure PIN is required for all active vendors and provided directly to the payee's authorized financial registration contact via email. Information is not shared with anyone outside of OCME.

### **F. Witness Information for State of Oklahoma court testimony**

i. District Attorney offices collect the following PII to perform witness background checks:

- a. Name (Employee)
- b. Date of birth

ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

ii. The PII is not shared with anyone outside of OCME.

### **G. Decedent Records**

i. Decedent medical records are not released according to O.S. 63, Section 931-954.

- a. Available Personnel Identifiable Information as available and pertinent to the death.

ii. The PII collected is stored by OCME in a manner consistent with the State's security policy and applicable regulatory requirements.

ii. The PII is not shared with anyone outside of OCME.

OCME complies with the Oklahoma Open Records Act, 51 OS §24A.1 et seq. In accordance with said law, some records referenced in this document must be made available for review and copying upon request. Where required or allowed by law, particular elements of PII (such as social security numbers, credit information or birthdates) will be redacted before making the records available. OCME will also share PII in response to a properly issued Court Order or subpoena.