OAKLAND COUNTY SHERIFF'S OFFICE

Policies and Procedures

NUMBER	DATE
350	November 13, 2018

SUBJECT: NON-DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION, PROTECTED HEALTH INFORMATION, AND CRIMINAL JUSTICE INFORMATION

Distribution: L, N.

REFERENCE:

Replaces and Rescinds P&P 334 dated February 21, 2018

POLICY

It shall be the policy of the Oakland County Sheriff's Office that the disclosure of Personally Identifiable Information (PII), Protected Health Information (PHI), or Criminal Justice Information (CJI) relating to any employee, contracted worker, victim, witness, suspect, arrestee, other individual or entity is prohibited unless there is a specific law enforcement purpose also referred to as a determined "need to know"; the information is needed by another criminal justice agency; or it is required by law to be disclosed. Personnel are expressly prohibited from the disclosure or discussion of PII, PHI, or CJI of a confidential nature, information that might violate the right to privacy of an individual. Unless specifically authorized, no information will be released without a request in writing from the person/agency seeking the information.

PURPOSE

The nature of police work requires specific information to remain confidential because of laws protecting individual rights and the need to protect certain operating procedures of the agency. This directive provides general guidelines regarding employee responsibilities in maintaining confidentiality of information.

PROCEDURES

1.0 Disclosure of information to other members of the Sheriff's Office will be on a need-to-know basis only. Work papers and documents within an office, on or in a desk, or computer files and disks are not for general viewing and all members are prohibited from attempting to observe or read such papers.

1.1 Personnel shall not photograph or record, by any means including the use of personal devices, any official police action or activity including but not limited to, vehicle or foot pursuits, use of force, or crime scenes except as is necessary in the official performance of their duties. Personnel shall not make any such recordings with their personally owned equipment for their personal use. All recordings of such activities made by personnel

during the official performance of their duties shall be the property of the Oakland County Sheriff's Office and the dissemination shall be in accordance with Sheriff's Office established procedures.

1.2 Employees will not maintain PII, PHI, or CJI including duplicate copies of information on personal media storage devices such as phones, tablets, thumb drives, cloud storage, personal email, CD's, DVD's, etc).

1.3 This Directive is not intended to restrict the flow of information within the Sheriff's Office, but is necessary to preserve the confidentiality of information.

2.0 PERSONALLY IDENTIFIABLE INFORMATION

2.1 The definition of Personally Identifiable Information is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Any data maintained by the Sheriff's Office, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII.

2.2 Employees shall make every effort to safeguard individuals PII so that it is not compromised.

3.0 PROTECTED HEALTH INFORMATION

3.1 In performing their employment duties, employees will directly or indirectly gain access to PHI. Employee must be aware that the PHI is protected from disclosure by various applicable federal and state laws, rules and regulations and other pertinent statutes and regulations.

3.2 Under the US Health Insurance Portability and Accountability Act (HIPAA), PHI that is linked based on the following list of 18 identifiers must be released only for permissible law enforcement purposes:

a. Names
b. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
c. Dates (other than year) directly related to an individual
d. Phone numbers
e. Fax numbers
f. Email addresses
g. Social Security numbers
h. Medical record numbers

i. Health insurance beneficiary numbers
j. Account numbers
k. Certificate/license numbers
l. Vehicle identifiers and serial numbers, including license plate numbers
m. Device identifiers and serial numbers
n. Web Uniform Resource Locators (URLs)
o. Internet Protocol (IP) address numbers
p. Biometric identifiers, including finger, retinal and voice prints
q. Full face photographic images and any comparable images
r. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

4.0 CRIMINAL JUSTICE INFORMATION (CJI)

4.1 Review and adhere to Policy & Procedures 066 and 223 regarding Disclosure of Information Received through the Law Enforcement Information Network (LEIN).

4.2 Disclosure of information obtained via other Criminal Justice resources including CJI relating to specific crimes.

4.3 Employees shall not release CJI from law enforcement reports, video or audio recordings, information obtained by using CJI vendor resources, any information obtained using CLEMIS programs, or information obtained from resources of other Law Enforcement agencies.

4.4 Employees should refer to Policies and Procedures or related Orders regarding the following for specific limitations:

a. Sexual Assault Investigations
b. Sexual Offender Registration
c. Release of Records via a valid F.O.I.A. request
d. Other Policies and Procedures or Orders that may have specific limitations

4.5 Questions regarding Records relating to requests involving Open Investigations/Cases should be referred to the Officer in Charge of the case or the Records Unit Supervisor.

5.0 NON-DISCLOSURE AGREEMENT

5.1 In order to ensure that all employees are aware of their responsibilities when handling PII, PHI, and CJI, employees shall sign the attached Non-Disclosure agreement. Each employee will be given a copy of the signed agreement and the original shall be stored in the Personnel file archive.

5.2 As outlined in the Non-Disclosure agreement, violations of this Policy and Procedure may result in disciplinary or legal action.

6.0 SUSPECTED PRIVACY INCIDENT REPORTING PROCEDURES

6.1 If any member of the Sheriff's Office detects a suspected privacy incident, they shall immediately notify their commanding officer/supervisor.

6.2 Once made aware of a suspected privacy incident, the commanding officer/supervisor shall ensure that a Suspected Privacy Incident Report form is filled out and immediately forwarded to the Sheriff's Office Privacy Officer in the Technology, Information, and Innovation Division (TII). (See the Suspected Privacy Incident Report form attached to this policy).

6.3 If the suspected privacy incident involves health information, the OCSO Privacy Officer shall notify the TII Captain or designated leadership, who will inform the HIPAA Privacy Officer. The HIPAA Privacy Officer will initiate investigation per Section 1.07 of the HIPAA Countywide Procedures.

6.4 Once the Suspected Privacy Incident Report form is received by the Privacy Officer, he or she will immediately notify the TII Captain. An investigation will be performed within OCSO and respective OC departments to determine if the suspected privacy incident is a breach. If determined to be a breach, the report shall be forwarded to any and all county, state, or federal agency that is required to receive it based on the nature of the breach.

6.5 If the suspected incident derives from an electronic source (email, web traffic, file share, etc.) the OCSO Privacy Officer will work with the TII Captain to ensure a cybersecurity incident is logged in Service Center (or emailed to servicecenter@oakgov.com for triage and remediation as necessary from Information Technology).

6.4 A copy of a Suspected Privacy Incident Report and subsequent remediation shall be securely saved for a period of 7 years from the date of the incident was discovered and closed.

Michael J. Bouchard
Sheriff

CWW/ses/tss

NON-DISCLOSURE OF PERSONAL PROTECTED INFORMATION AGREEMENT

This Non-Disclosure of Personal Protected Information Compliance Agreement (hereinafter "Agreement") is entered into by and between _____ (hereinafter "Employee", which also include volunteers) and the Oakland County Sheriff's Office, (hereinafter referred to as "Employer") as of this day the _____ of _____ 20_____, in regard to the following facts:

A. Employer is a Law Enforcement Agency responsible for obtaining, processing, and retaining Personally Identifiable Information (PII), Protected Health Information (PHI), and Criminal Justice Information (CJI). This information is sensitive and must be safeguarded under various laws and rules and regulations such as The Privacy Act of 1974, Title 18 of the US Code (section 1028d(7), The Health Insurance Portability and Accountability Act of 1996 (HIPAA), FBI CJIS Policy, etc.

B. In performing their employment duties, Employee acknowledges that they will directly or indirectly gain access to PII, PHI & CJI. Employee further acknowledges that the PII, PHI, & CJI is protected from disclosure by various applicable federal and state laws, rules and regulations such as FBI CJIS Policy and other pertinent statutes and regulations, the violation of which is the basis of both civil and criminal liability.

C. As a condition of employment, "Employees" and staff members including volunteers must agree to maintain the confidentiality of all PII, PHI, and CJI as set forth in this Agreement.

NOW, THEREFORE, Employee agrees as follows:

1. **Term of Agreement.** This agreement shall commence on the date set forth in the first paragraph above and the obligations herein shall continue in effect so long as Employee uses, discloses, creates, or otherwise possesses any PII, PHI, or CJI created or received during their employment with Employer and until all PII, PHI, and CJI created or received during their employment with Employer has been returned to Employer.

2. **Use of PII, PHI, and CJI by Employee.** Employee may only use and disclose PII, PHI, and CJI created or received by them during the term of their employment, on behalf of Employer for the purposes of carrying out their duties with the Oakland County Sheriff's Office.

3. **Maintenance of Security and Privacy of PII, PHI, and CJI.** Employee hereby agrees to maintain the security and privacy of all PII, PHI, and CJI in a manner consistent with state and federal laws and regulations. Employee further agrees to not use or disclose PII, PHI, and CJI except as expressly permitted by this Agreement, applicable laws or regulations, or departmental policies and procedures, orders, and/or directives given by a Command Officer so long as the directive from a Command Officer is not contrary to laws, rules and regulations, departmental orders, and/or policies and procedures. Employee further agrees to use appropriate safeguards to prevent use or disclosure of PII, PHI, and CJI not permitted by this Agreement, applicable laws or rules and regulations (such as HIPAA, the FBI CJIS policy, etc).

4. **Reporting Unauthorized Disclosure of PII, PHI, and CJI.** Employee agrees to immediately report to Employer any unauthorized or inadvertent use or disclosure of PII, PHI,

and/or CJI by Employee, Employer's other employees, Employer's subcontractors, or any other person or persons which occur while Employee is performing services within the scope of their employment with Employer.

5. **Disciplinary Action Up To and Including Termination of Employment upon Breach of Agreement.** Employer may immediately discipline an employee including taking action that may include termination of Employee's employment if Employer determines that Employee has breached a material term of this Agreement. Employer's remedies for breach of this Agreement are cumulative, and termination of Employee's employment shall not preclude Employer from exercising any other remedy, whether at law, equity, or otherwise.

6. **Return of PII, PHI, and CJI upon Termination of Employment.** Upon termination of Employee's employment, Employee shall return all PII, PHI, and/or CJI regardless of the form in which it is being stored, acquired, created, or received by Employee on account of employer or while Employee was performing services within the scope of their employment with Employer. Employee further agrees that they shall retain no copies of any such PII, PHI, or CJI. The duties of Employee hereunder to maintain the security and privacy of PII, PHI, and CJI shall survive the termination of Employee's employment with Employer.

MY SIGNATURE BELOW ATTESTS to the fact that I have read, understand, and agree to be legally bound to all of the above terms.

Signed in the state of Michigan, this day of_____, 20__.

_____

OCSO Employee/Staff Signature

_____

OCSO Employee/Staff Printed Name

OAKLAND COUNTY SHERIFF'S OFFICE
SUSPECTED PRIVACY INCIDENT REPORT

Incident Reported by:			
Name:		**Supervisor:**	
Email:		**Email:**	
Phone:		**Phone:**	
Agency/Sub-agency/Component:			

Summary of the Incident:	
Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including: a. A description of the parties involved in the incident; b. The physical or electronic storage location of the information at risk; c. If steps were immediately taken to contain the breach; d. Whether the incident is an isolated occurrence or a systematic problem; e. Who conducted the investigations of the breach, if applicable; and f. Any other pertinent information.	
Date and Time of the Incident:	
Location of Incident:	

Type of Incident:			
Lost Information or Equipment	◯ Yes ◯ No	**Unauthorized Disclosure** (e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, disclosing documents publicly with sensitive information not redacted)	◯ Yes ◯ No
Stolen Information or Equipment	◯ Yes ◯ No	**Unauthorized Access** (e.g., an unauthorized employee or contractor accesses information or an information system)	◯ Yes ◯ No
Unauthorized Equipment (e.g., using an unauthorized personal device, server, or email account to store PII)	◯ Yes ◯ No	**Unauthorized Use** (e.g., employee with agency-authorized access to database or file accesses and uses information for personal purposes rather than for official purposes)	◯ Yes ◯ No

Storage Medium:			
Laptop or Tablet	Yes ◯ No ◯	**Smartphone**	Yes ◯ No ◯
Desktop	Yes ◯ No ◯	**Paper files**	Yes ◯ No ◯
External Storage Device	Yes ◯ No ◯	**External Storage Device** (e.g., CD, DVD, USB Drive, etc.)	Yes ◯ No ◯
IT System (Intranet/Shared Drive)	Yes ◯ No ◯	**Oral Disclosure**	Yes ◯ No ◯
Email:			
Other:			

Reported to US-CERT, Law Enforcement, or Congress	
Reported to US-CERT Yes ◯ No ◯ **Reported to Law Enforcement** Yes ◯ No ◯ **Reported to Congress** Yes ◯ No ◯	**If yes, complete the following:**
Name:	

Title:			
Email:			
Phone:			
Agency/Component		**Agency:**	
Date and Time of the Report:			

Number of Individuals and Safeguards	
Number of individuals potentially affected by the incident?	
Was the information unstructured? (e.g., open fields on a form or survey)	**Yes** ◯ **No** ◯
Was the information encrypted (see Section VII.E.2. of this Memorandum)	
Does a duplicate set of the potentially compromised information exist?	**Yes** ◯ **No** ◯

Additional Information	
Internal incident (e.g., within the agency's network), external, both, or unknown?	
What counter measures, if any, were enabled when the incident occurred?	
What steps, if any, have already been taken to mitigate potential harm?	
Do you have knowledge that any information involved in the incident was intentionally stolen or misused?	**Yes** ◯ **No** ◯

Data Elements and Information Types

Place a mark by the data elements or information types were a part of the incident

Identifying Numbers			
	Social Security number		Truncated or Partial Social Security number
	Driver's License Number		License Plate Number
	DEA Registration Number		File/Case ID Number
	Patient ID Number		Health Plan Beneficiary Number
	Student ID Number		Federal Student Aid Number
	Passport number		Alien Registration Number
	DOD ID Number		DOD Benefits Number
	Employee Identification Number		Professional License Number
	Taxpayer Identification Number		Business Taxpayer Identification Number (sole proprietor)
	Credit/Debit Card Number		Business Credit Card Number (sole proprietor)
	Vehicle Identification Number		Business Vehicle Identification Number (sole proprietor)
	Personal Bank Account Number		Business Bank Account Number (sole proprietor)
	Personal Device Identifiers or Serial Numbers		Business device identifiers or serial numbers (sole proprietor)
	Personal Mobile Number		Business Mobile Number (sole proprietor)

Biographical Information					
	Name (including nicknames)		Gender		Race
	Date of Birth (Day, Month, Year)		Ethnicity		Nationality
	Country of Birth		City or County of Birth		Marital Status
	Citizenship		Immigration Status		Religion/Religious Preference
	Home Address		Zip Code		Home Phone or Fax Number
	Spouse Information		Sexual Orientation		Children Information
	Group/Organization Membership		Military Service Information		Mother's Maiden Name
	Business Mailing Address (sole proprietor)		Business Phone or Fax Number (sole proprietor)		Global Positioning System (GPS)/Location Data
	Personal e-mail address		Business e-mail address		Employment Information
	Personal Financial Information (including loan information)		Business Financial Information (including loan information)		Alias (e.g., username or screenname)
	Education Information		Resume or curriculum vitae		Professional/personal references

Biometrics/Distinguishing Features/Characteristics					
	Fingerprints		Palm prints		Vascular scans
	Retina/Iris Scans		Dental Profile		Scars, marks, tattoos
	Hair Color		Eye Color		Height
	Video recording		Photos		Voice/Audio Recording
	DNA Sample or Profile		Signatures		Weight

Medical/Emergency Information (select all that apply)					
	Medical/Health Information		Mental Health Information		Disability Information
	Workers' Compensation Information		Patient ID Number		Emergency Contact Information

Device Information					
	Device settings or preferences (e.g., security level, sharing options, ringtones)		Cell tower records (e.g., logs, user location, time, etc.)		Network communications data

Specific Information/File Types					
	Taxpayer Information/Tax Return Information		Law Enforcement Information		Security Clearance/Background Check Information
	Civil/Criminal History Information/Police Record		Academic and Professional Background Information		Health Information
	Case files		Personnel Files		Credit History Information

Additional Information