

DATA USE AGREEMENT

between

**THE STATE OF NEW JERSEY
DEPARTMENT OF HEALTH**

and

**THE STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC SAFETY**

This Data Use Agreement (Agreement) sets forth the terms under which the STATE OF NEW JERSEY, DEPARTMENT OF HEALTH (NJDOH), and the STATE OF NEW JERSEY, DEPARTMENT OF LAW AND PUBLIC SAFETY (NJDLPS), (individually, a “Party” or, collectively, the “Parties”) agree to share certain data and datasets that are individually collected and maintained by each Party.

I. PURPOSES

The purposes of this Agreement are to:

- A. Provide NJDLPS with a limited Emergency Medical Services (EMS) response dataset involving the EMS administration of naloxone to:
 1. Enable NJDLPS’s Division of State Police (NJSP) to support the NJSP Drug Monitoring Initiative (DMI), Overdose Detection Mapping Application Program (ODMAP), and public health efforts including law enforcement situational awareness in order to lessen and prevent the threat to the public of overdoses due to possible opioid use or abuse, identify those who are being disproportionately affected, as well as to administer first aid; and
 2. Enable NJDLPS’s Office of the New Jersey Coordinator of Addiction Response & Enforcement Strategies (NJ CARES) to support the Integrated Drug Awareness Dashboard (IDAD), an inter-agency analytics platform that allows State agencies engaged in fighting the opioid epidemic to exchange and analyze data and obtain a more comprehensive picture of the impact of the opioid crisis and thereby develop better informed strategies to combat it.
 3. Enable NJDLPS’s Office of Justice Data (OJD)—which works to ensure that policymaking across the NJDLPS is rooted in data and rigorous statistical analysis—to support and assess public safety and public health initiatives including, but not limited to,

examinations of (i) responses to potential mental health incidents, and (ii) locations of gun crime victims.

- B. Provide NJDOH with a limited dataset regarding the law enforcement administration of naloxone under the terms of New Jersey Attorney General Law Enforcement Directive No. 2014-2 Concerning Heroin and Opiate Investigations/Prosecutions to enable NJDOH to support the DMI, ODMAP, IDAD, and other public health efforts designed to lessen and prevent the threat to the public of overdoses of suspected opioids including its New Jersey Opioid Data Dashboard (DOH Dashboard), which uses interactive data visualizations to display opioid and other drug-related overdose indicators for public health practitioners, researchers, policy-makers, and the public, as well as to administer first aid.

II. PARTIES TO THE AGREEMENT

The Parties to this Agreement are the NJDOH and NJDLPS.

III. LEGAL AUTHORITY

- A. The NJDOH enters into this Agreement under the authority of the laws of the State of New Jersey, specifically N.J.S.A. 26:2H-1, the statute that authorizes NJDOH to collect patient data to carry out the work of the agency, and N.J.S.A. 26:1A-15, the statute that authorizes NJDOH to work collaboratively with other State agencies on matters affecting public health. The NJDOH also enters into this Agreement under the terms of N.J.S.A 26:2K-67 and N.J.S.A 26:2K-68 the statutes which require emergency medical services providers to report certain information to NJDOH in order for NJDOH to record and track data concerning types of medical emergencies for which emergency medical services are requested, response times for emergency medical services providers, patterns in the timing and location of requests for emergency medical services, patterns in the type or nature of emergency medical services provided, and patterns in dispatch and response activity.
- B. The NJDLPS enters into this Agreement in furtherance of its authority under N.J.S.A. 52:17A-1, *et seq.*, to protect the health, welfare, and public safety of New Jersey residents. The NJDLPS does so through the work of its sub-divisions, offices, and units including, but not limited to the NJSP, N.J.S.A. 53:1-1, *et seq.*, and NJ CARES. NJDLPS is authorized to work collaboratively with public and private entities on matters affecting public health, welfare, and safety.
- C. Notwithstanding the use of or reference to legal requirements, rules, or terms associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1996 (1996), neither Party considers itself to be a "covered entity" as defined in under 45 CFR 160.103. The use of HIPAA legal requirements, rules, or terms under this Agreement is intended only to adhere to a recognized framework for information sharing.

D. Responsible Officials

1. The NJDOH official responsible for implementing this Agreement is the Acting Commissioner of NJDOH or whomever she/he authorizes to act on her/his behalf in this matter.
2. The NJDLPS official responsible for implementing this Agreement is the Attorney General of New Jersey or whomever he/she authorizes to act on his/her behalf in this matter.

IV. DEFINITIONS

- A. "Breach" shall have the same meaning given under 45 CFR 164.402.
- B. "Breach of Security" shall have the same meaning given under N.J.S.A. 56:8-161.
- C. "Disclose" or "Disclosure" means the release of data in accordance with the terms of this Agreement.
- D. "Emergency Medical Services" or "EMS" means NJDOH licensed Advanced Life Support and all Basic Life Support agencies reporting naloxone deployment to NJDOH.
- E. "Encryption" or "Encrypt" means a technology-aided process that renders information unreadable, undecipherable, or otherwise unusable by an unauthorized person.
- F. "Opioid" means drugs (prescription or illicit) that either are derived from opium or that are chemically (synthetically) produced to possess the same properties as an opiate, including but not limited to heroin.
- G. "Personally Identifiable Information" (PII) shall have the same meaning set forth in the Statewide Information Security Manual (https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf), namely, 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.
- H. "Protected Health Information" (PHI) shall have the same meaning given under 45 CFR 160.103.

V. RESPONSIBILITIES OF THE PARTIES

A. NJDLPS shall be responsible for the following:

1. Maintaining Data Confidentiality Agreements, attached to this Agreement as Attachment 1, executed by NJDLPS employees, contractors, and agents who have access to NJDOH data received pursuant to this Agreement.
2. Using appropriate safeguards to maintain and ensure the confidentiality, privacy, and security of NJDLPS data, which may be tagged as law enforcement sensitive, transmitted to NJDOH pursuant to this Agreement until such NJDLPS data is received by NJDOH.
3. Ensuring that internal security measures currently in place at NJDLPS comply with the confidentiality provisions set forth in this Agreement that are established to prevent the unauthorized disclosure of NJDOH data received pursuant to this Agreement.
4. Cooperating with NJDOH if NJDOH is audited with regard to program confidentiality, or if NJDOH is required to undergo a compliance review. This includes permitting site and record inspections as discussed in Section VII(J), below.
5. Ensuring that authorized NJSP employees, contractors, and agents provide NJDOH with the NJSP datasets listed in Section VI(A) through either direct input into NJDOH's Electronic Patient Care Reporting System or secure file transfer protocol. NJSP shall provide these datasets to the NJDOH on a daily basis. The daily reports shall be provided as of the effective date of this Agreement. A copy of the Naloxone Deployment Reporting Form that NJSP uses to populate the datasets listed in Section VI(A) is attached for reference as Attachment 3.
6. On the fifteenth day of each month, NJSP shall provide to NJDOH all of the information collected by NJSP in the datasets listed in Section VI(A) for the preceding month in order to capture any delayed reporting of such information. NJSP may provide this information through a secure file transfer protocol or by directly entering the information into the NJDOH's Electronic Patient Care Reporting System. The first monthly report shall be provided on the fifteenth day of the first month following the execution of this Agreement.

B. NJDOH shall be responsible for the following:

1. Maintaining Data Confidentiality Agreements, attached to this Agreement as Attachment 2, executed by NJDOH employees, contractors, and agents

who have access to NJDOH and NJDLPS data received pursuant to this Agreement.

2. Using appropriate safeguards to maintain and ensure the confidentiality, privacy, and security of NJDOH data, which may include PII and PHI, transmitted to NJDLPS pursuant to this Agreement until such NJDOH data is received by NJDLPS.
3. Ensuring that internal security measures currently in place at NJDOH comply with the confidentiality provisions set forth in this Agreement that are established to prevent the unauthorized disclosure of NJDLPS data received pursuant to this Agreement.
4. Cooperating with NJDLPS if NJDLPS is audited with regard to program confidentiality, or if NJDLPS is required to undergo a compliance review. This includes permitting site and record inspections as discussed in Section VII(J) below.
5. Ensuring authorized NJDOH employees, contractors, and agents provide NJDLPS with the NJDOH datasets listed in Section VI(A), through either granting NJDLPS limited access to NJDOH's Electronic Patient Care Reporting System or secure file transfer protocol generated by NJDOH's Electronic Patient Care Reporting System. NJDOH shall provide these datasets to NJDLPS on a daily basis. The daily reports shall be provided as of the effective date of this Agreement.
6. On the fifteenth day of each month, NJDOH shall provide to NJDLPS all of the information collected by NJDOH in the datasets listed in Section VI(A) for the preceding month in order to capture any delayed reporting of information. NJDOH may provide this information through a secure file transfer protocol generated by NJDOH's Electronic Patient Care Reporting System or by granting NJSP limited access to NJDOH's Electronic Patient Care Reporting System. The first monthly report shall be provided on the fifteenth day of the first month following the execution of this Agreement.

VI. DATA SHARING

- A. NJDOH and NJDLPS shall provide each other with the following datasets regarding naloxone deployments from their respective reporting mechanisms, to the extent they exist.

Element	NEMESIS code
Age	ePatient.15
Gender	ePatient.13
Race	ePatient.14
Ethnicity	ePatient.14

Date of Incident	eTimes.03			
Scene Incident Street Address (needed for cross reference of Scene GPS)	eScene.15			
Scene Incident City (needed for cross reference of Scene GPS)	eScene.17			
Scene Incident County (needed for cross reference of Scene GPS)	eScene.21			
Incident ZIP Code (needed for cross reference of Scene GPS)	eScene.19			
Patient's Home Zip Code	ePatient.09			
Scene GPS Location	eScene.11			
Situation Primary Complaint Statement List	eSituation. 04			
Alcohol/Druq Use Indicators	elnjury.01			
Medication Given	eMedication.03			
Incident Patient Disposition	eDisposition.12			
Cause of Injury	elnjury.01			
Number of doses of naloxone administered	eMedications.05			
Disposition Destination Delivered Transferred To (i.e., hospital, if any, to which the person was transported)	eDisposition. 01			
Other EMS or Public Safety Agencies at Scene	eScene.02			
Medication Administered Prior to this Unit's EMS Care (i.e., whether a bystander administered the naloxone)	eMedications.02			
Injury Location of Patient in Vehicle	elnjury.06			
Drug Stamp (when supplied by law enforcement agencies to NJSP or EMS to DOH, respectively)	NA			
Incident ID (used for cross referencing)	eResponse.01			
Agency Name (used for cross referencing)	dAgency.03			
Vendor Name (used for cross referencing)	eRecord.02			
Response to Medication	eMedications.07			
Level of Care of This Unit	eResponse.15			
Provider's Primary Impression	eSituation.11			
Situation Primary Symptom	eSituation.09			
Incident Complaint Reported By Dispatch	eDispatch.01			
EMS Response Number	eResponse.04			
Provider secondary impression	esituation.12	CRITERIA		
eDispatch.01 - Complaint Reported by Dispatch	eDispatch.01	GSW/Penetrating Trauma	Psych	OD
Mechanism of Injury	elnjury.02			
Trauma Center Criteria	elnjury.03			
Narrative	enarrative.01			
Unit Notified by Dispatch Date/Time	eTimes.03			
Unit En Route Date/Time	eTimes.05			

Unit Arrived on Scene Date/Time	eTimes.06
Arrived at Patient Date/Time	eTimes.07
Unit Left Scene Date/Time	eTimes.09
Arrival at Destination Landing Area Date/Time	eTimes.10
Patient Arrived at Destination Date/Time	eTimes.11
Patient Evaluation/Care	eDisposition.28
Transport Disposition	eDisposition.30

- B. Notwithstanding the requirement to mutually share information in Section VI(A), the following exceptions apply:
1. NJDLPS reserves the right to withhold any or all information contained within its "Drug Stamp" dataset when in NJDLPS's sole determination that information is related to an active law enforcement investigation.
 2. The "Vendor Name" dataset is only shared from NJDOH to NJDLPS. The Vendor Name data set is "the name of the vendor, manufacturer, and developer who designed the application that created the record" (in reference to National Emergency Services Information Systems "NEMESIS" definition).
- C. The Parties agree that the data received pursuant to this Agreement shall be used only for the purposes authorized in this Agreement. The Parties further agree that access to each other's data is limited to the datasets listed in this Agreement and only to the extent that such data access is necessary to accomplish the purposes of this Agreement.
- D. NJDLPS permissible uses of NJDOH datasets
1. NJDLPS may use NJDOH data received pursuant to this Agreement for public health purposes only, which includes but is not limited to law enforcement situational awareness through the DMI, ODMAP, IDAD, OJD, and first aid.
 2. NJDLPS may link the NJDOH data received pursuant to this Agreement with other NJDLPS data elements to create aggregate reports for public health purposes regarding opioid overdoses or suspected overdoses, responses to potential mental health incidents, and issues regarding gun violence. These reports may be made available to NJSP, law enforcement, and public health entities for public health purposes only, which include law enforcement situational awareness.
 3. NJDLPS is authorized to geocode, map, and overlay NJDOH data received pursuant to this Agreement for use in the ODMAP, IDAD, DMI, and OJD reports for public health purposes, including but not limited to:

- a. Weekly Suspected Opioid Overdose Summaries, which analyze heroin stamps seized, naloxone administrations, and drug fatalities;
 - b. Statewide Drug Harm Assessments, which analyze the seizure of heroin and opioids, naloxone administrations, drug fatalities, drug arrests, and shooting trends and patterns on a Statewide basis;
 - c. County Drug Harm Assessments, which analyze the seizure of heroin and opioids, naloxone administrations, drug fatalities, drug arrests, and shooting trends and patterns on a county-by-county basis; and
 - d. Quarterly Drug Trends, which analyze the seizure of heroin and opioids, naloxone administrations, drug fatalities, drug arrests, and shooting trends and patterns.
4. OJD may use NJDOH data received pursuant to this Agreement to support and assess public safety and public health initiatives including, but not limited to, examinations of responses to potential mental health incidents, and the locations of gun crime victims, in furtherance of its charge to ensure that policymaking is rooted in data and rigorous statistical analysis.

E. NJDOH permissible uses of NJDLPS datasets

1. NJDOH may use NJDLPS data received pursuant to this Agreement for public health purposes only, which include EMS situational awareness.
2. NJDOH may combine the NJDLPS data received pursuant to this Agreement with other NJDOH data to create aggregate reports for public health purposes regarding suspected opioid overdoses. These reports may be made available to public health entities for public health purposes only, which include EMS situational awareness.
3. NJDOH may use NJDLPS data received pursuant to this Agreement for integration the DOH Dashboard.
4. NJDOH is authorized to geocode, map, and overlay NJDLPS data received pursuant to this Agreement for public health purposes only.
5. Notwithstanding the permissible uses of NJDLPS datasets as described in this section, NJDOH agrees that any "Drug Stamp" data received from NJDLPS pursuant to Section VI(A) shall be for internal NJDOH use only, and, with the exception of NJDLPS, shall not be released to any third party for any purpose whatsoever.

VII. CONFIDENTIALITY & RESTRICTIONS ON THE USE OF DATA

A. Data Confidentiality

1. The Parties recognize that confidentiality of the data received pursuant to this Agreement is of paramount importance and must be observed except where disclosure is permitted by this Agreement or required by State or federal law, or court order (see Section IX). All data exchanged pursuant to this Agreement shall be conducted in a manner consistent with applicable State and federal laws.
2. The Parties agree to take all necessary steps to protect the privacy of the data received pursuant to this Agreement by complying with the provisions that govern the handling of confidential information as applicable to their respective shared datasets.
3. For the purposes of this Agreement, NJDLPS agrees to treat NJDOH data received pursuant to this Agreement in a manner consistent with the legal requirements of HIPAA.
4. NJDOH agrees to treat NJDLPS data received pursuant to this Agreement as law enforcement sensitive and limit access, use, and dissemination only to authorized individuals with a need-to-know and right-to-know consistent with the purposes authorized under this Agreement.

B. Party Privacy and Confidentiality

1. Each Party's access to and use of data received pursuant to this Agreement shall be restricted to a Party's employees, contractors, or agents whose access, use, or dissemination of data received pursuant to this Agreement is necessary to perform their official duties and in connection with the purposes of this Agreement.
2. Each Party shall advise its employees, contractors, and agents who are authorized to have access to data received pursuant to this Agreement of the confidential nature of the information, the safeguards required to protect the information, the permissible uses of information established pursuant to this Agreement, and the potential discipline and civil and criminal sanctions for noncompliance.
3. The Parties agree to require their respective employees, contractors, and agents to execute Data Confidentiality Agreements (Attachments 1 and 2 to this Agreement, as applicable) in order for them to access, use, or disclose data received pursuant to this Agreement.

C. Use and Disclosure

1. Unless otherwise permitted in this Agreement, no Party employee, contractor, or agent may disseminate data received pursuant to this Agreement except to authorized employees, contractors, or agents who, by executing Data Confidentiality Agreements, are specifically authorized to receive such data.
2. Unless otherwise permitted in this Agreement, the access, use, and dissemination of data received pursuant to this Agreement and to any records created from such data shall be restricted to only a Party's employees, contractors, or agents whose access to and use of such data are necessary to perform their official duties in connection with the purpose of this Agreement.
3. The Parties agree that they shall not disclose data received pursuant to this Agreement to any unauthorized individuals, which may include a Party's employees, contractors, or agents but who are not authorized to access or use the data received pursuant to this Agreement.
4. The Parties agree that they shall not make public or publish any information received pursuant to this Agreement that constitutes PII.
5. Each Party shall process the data received pursuant to this Agreement to protect the confidentiality of the data, and in a method to ensure that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means.
6. Each Party agrees to make its comprehensive written information privacy and security programs, as well as internal practices, books, and records, including policies and procedures relating to the use and disclosure of data received pursuant to this Agreement, available upon request of the other Party. The responding Party shall make available the requested items to the requesting Party within 30 days of such request.

D. Secure Destruction

1. The Parties shall retain data received pursuant to this Agreement in accordance with applicable record retention policies and schedules for destruction. When a Party destroys data received pursuant to this Agreement, that Party shall notify the other Party in writing of such destruction. The Parties also agree to destroy or archive until destruction is required, as applicable, all data received from the other Party pursuant to this Agreement within 30 days after the Agreement's termination date.

E. Training

1. The Parties shall train their respective employees, contractors, and agents who are granted access to data received pursuant to this Agreement regarding the confidentiality of such information, the safeguards required to protect the information, and the potential civil and criminal sanctions for non-compliance under applicable federal and State laws. Such training shall include:
 - a. Implementation of and adherence to the Agreement in a Party's work environment.
 - b. The use or disclosure of data received pursuant to this Agreement.
 - c. Procedures for reporting violations of the use of data received pursuant to this Agreement including the potential for corrective action against employees, contractors, or agents who violate any provisions of the Agreement.
 - d. Provide, within 30 days of employment or joining a Party's workforce, privacy and security awareness training to each new employee, contractor, or agent whose job responsibilities include accessing or using data received pursuant to this Agreement.
 - e. Provide ongoing reminders of the privacy and security safeguards in this Agreement to all employees and workforce who access, use, or disclose data received pursuant to this Agreement. These reminders shall occur not less than once every two weeks.
2. The Parties shall maintain records that show receipt of the initial privacy and security training, which shall include the name of each of employee, contractor, or agent who completed the training and the date of the training. The Parties shall retain these records for three years after the completion of the training, or in accordance with the time period established in an applicable record retention schedule, whichever is longer.

F. Physical Security

1. The Parties agree to safeguard the data that they receive pursuant to this Agreement through the use of physical, technical, and administrative methods to prevent loss, theft, or inadvertent disclosure, or use or disclosure other than as provided for through this Agreement.
2. Each Party shall ensure that the data received pursuant to this Agreement is used and stored in an area that is physically secured, including from

access by unauthorized persons during working hours and non-working hours. The Parties shall secure all areas of their respective facilities where their employees, contractors, and agents access, use, or disclose data received pursuant to this Agreement. The Parties shall ensure that access to these secured areas is granted only to authorized individuals who display official identification and use key cards, authorized door keys, or other equivalent access control.

3. Each Party shall be responsible for issuing identification badges to its own employees, contractors, and agents, and require display of those badges at all times within their respective facilities where data received pursuant to this Agreement is accessed, used, or disclosed.
4. Each Party shall store physical records containing data received pursuant to this Agreement in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices. The Parties shall provide such secured storage in all facilities where data received pursuant to this Agreement is accessed or stored, including facilities that are multi-use, meaning that, where Party and non-Party functions are conducted in one building, whether or not they are segregated from each other. The Parties shall develop and maintain policies that direct their respective employees, contractors, and agents not to leave records (paper or electronic) with data received pursuant to this Agreement unattended at any time in vehicles or airplanes and not to check such records in baggage on commercial airplanes.
5. The Parties agree to use all necessary measures to prevent unauthorized individuals from accessing or viewing data received pursuant to this Agreement.

G. Computer Security Safeguards

1. The Parties shall encrypt all electronic files that contain data received pursuant to this Agreement when stored electronically, whether in databases, portable computer devices, or removable storage devices (for example, USB thumb drives, floppies, CD/DVD, portable hard drives, etc.) in accordance with New Jersey Office of Information Technology (NJOIT) Policy No. 18-02-NJOIT, and comply in all other respects with OIT policies and guidance including the Statewide Information Security Manual ([https://www.nj.gov/it/docs/ps/NJ Statewide Information Security Manual .pdf](https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf)).
2. The Parties shall encrypt portable computer devices, such as but not limited to laptops and notebook computers, that process or store data received pursuant to this Agreement. Each Party agrees to use an encryption tool that uses a full-disk standard unless otherwise approved by NJOIT.

3. The Parties shall ensure that only the minimum necessary amount of data received pursuant to this Agreement is downloaded to an authorized laptop or hard drive and when only absolutely necessary to accomplish the purposes of this Agreement.
4. The Parties shall ensure that all email sent outside of their respective secured e-mail environments that includes data received pursuant to this Agreement is sent and delivered using an encrypted process as established by NJOIT.
5. The Parties shall ensure that all workstations, laptops, and other electronic systems that process or store data received pursuant to this Agreement have installed and keep current an anti-virus software solution as supplied by the Party and NJOIT.
6. The Parties shall ensure that all workstations, laptops, and other electronic systems that process or store data received pursuant to this Agreement maintain current software and system security updates.
7. The Parties shall ensure that all data received pursuant to this Agreement is permanently deleted from their respective computer systems, backups, and removable media devices when subject to destruction as part of an applicable records retention policy.
8. The Parties shall ensure that their respective employees, contractors, or agents who are granted remote access to the data received pursuant to this Agreement only do so through an encrypted session protocol and in accordance with NJOIT policy and guidance.

H. System Security Controls

1. The Parties shall ensure that their respective systems containing data received pursuant to this Agreement provide an automatic timeout after no more than 15 minutes of inactivity.
2. The Parties shall ensure that their respective systems containing data received pursuant to this Agreement display a warning banner stating that the data is confidential, systems are logged, and system use is for business purposes only. Users shall be required to agree with the above requirements to access the data received pursuant to this Agreement.
3. The Parties shall ensure that their respective systems containing data received pursuant to this Agreement log and maintain user authentication successes and failures. Such a system shall log all data changes and system accesses conducted by all users (including all levels of users,

system administrators, developers, and auditors). The system shall have the capability to record data access for specified users when requested by authorized management workforce. The Parties shall maintain a logbook of all system changes and be available for review by the authorized internal management of each agency.

4. The Parties shall ensure that their respective workstations containing data received pursuant to this Agreement require role-based access controls for all user authentications.
5. The Parties shall ensure that their respective data transmissions over networks outside of their control are encrypted end-to-end using a software product approved by NJOIT. The Parties shall encrypt transmissions of data received pursuant to this Agreement at the minimum of 256 bit AES or 3DES (Triple DES) if AES is unavailable.
6. The Parties shall ensure that their respective computer and network systems that are accessible via the Internet and may allow for access to data received pursuant to this Agreement use a comprehensive network monitoring solution. This solution should allow for analytics to identify potential malicious activity and provide alerts for events that need to be further evaluated by the Party that owns the device when notified of such activity.

I. Audit Controls

1. Each Party shall conduct an annual system security review for its computer and network systems that process the data received pursuant to this Agreement. This review shall include administrative and technical vulnerability assessments.
2. The Parties shall ensure that their respective software application systems processing or storing data received pursuant to this Agreement include an automated audit trail, which includes the initiator of the request, the requestor's business purpose, and a time and date stamp for each access. These logs shall be read-only and maintained for a period of at least three years or in accordance with the time period established in an applicable record retention schedule, whichever is longer. Each Party agrees to develop an ongoing review of system logs for unauthorized access. Each Party further agrees to investigate anomalies through its review and take corrective action as warranted. The Parties agree to notify one another in writing of the outcomes of their respective investigations.
3. The Parties shall exercise management control and oversight over authorizing their respective individual users access to data received pursuant to this Agreement and issuing and maintaining access control

numbers and passwords to their respective employees, contractors, and agents.

J. Onsite Audit

1. Each Party agrees that, from time to time and upon reasonable notice, it shall permit the other Party or that Party's authorized contractors or agents to inspect its facilities, computer and network systems, books, records, and procedures to monitor compliance with this Agreement. In the event that a Party, in its sole discretion, determines that the other Party has violated any term of this Agreement it shall so notify the violating Party in writing. The violating Party shall promptly remedy such violation and shall certify the same in writing to the other Party.
2. The fact that a Party or its authorized contractors or agents inspect, fail to inspect, or have the right to inspect the other Party's facilities, computer and network systems, books, records, and procedures does not relieve that Party of its responsibilities to comply with this Agreement. A Party's (1) failure to detect, or (2) detection but failure to notify, or (3) failure to require remediation of any unsatisfactory practice shall not constitute acceptance of such practice or a waiver of a Party's enforcement rights under this Agreement.

K. Notification of Breaches

1. Unauthorized Acquisition; Immediate Notification

Each Party agrees to notify the other Party immediately upon the discovery of a Breach or Breach of Security regarding data received pursuant to this Agreement if the data was, or is reasonably believed to have been, acquired by an unauthorized person. The initial notification may be verbal but shall be confirmed in writing.

2. Security Incident; Notification within 24 Hours

Each Party agrees to notify the other Party within 24 hours upon the discovery of any suspected security incident, intrusion, loss, or unauthorized use or disclosure of data received pursuant to this Agreement. The initial notification may be verbal but shall be confirmed in writing.

3. New Jersey Data Breach Reporting

In addition to the requirements described in Sections VII(K)(1) & (2) above, the Parties agree to comply with the applicable provisions of N.J.S.A. 56:8-163. The Parties further agree that compliance with Sections VII(K)(1) & (2) above does not satisfy a Party's reporting requirement regarding N.J.S.A. 56:8-163.

4. Notification Contents

a. NJDLPS Notifications to NJDOH:

NJDLPS notifications to NJDOH during normal business hours, 8:00AM – 5:00PM, Monday through Friday, shall be submitted to the NJDOH Data Privacy Officer and the NJDOH Information Security Officer. Notifications outside of business hours shall be submitted to NJDOH by calling the NJDOH's OITS Help Desk.

NJDOH Data Privacy Officer
New Jersey Department of Health
P.O. Box 360
Trenton, NJ 08625
Email: privacy.officer@doh.nj.gov
Telephone: (609) 376-0972

NJDOH Information Security Officer
c/o: Office of Information Technology Services
New Jersey Department of Health
P.O. Box 360
Trenton, NJ 08625
Email: iso@doh.nj.gov
Telephone: NJDOH OITS Help Desk (609) 984-0224

b. NJDOH Notifications to NJDLPS:

NJDOH notifications to NJDLPS during normal business hours, 8:00AM – 5:00PM, Monday through Friday, shall be submitted to the NCC Help Desk, 800-NCC-HELP. Notifications outside of business hours shall be submitted to the Regional Operations and Intelligence Center at: 906-963-6951.

5. Notification Content

Breach and Breach or Security notifications shall include the following information:

- a. Contact and component information;
- b. Description of the breach or loss with scope, numbers of files or records;
- c. Type of equipment or media;
- d. Approximate time and location of breach or loss;

- e. Description of how the data was physically stored, contained, or packaged (for example, password protected, encrypted, locked briefcase, etc.);
 - f. Whether any individuals or external organizations should be contacted; and
 - g. Whether any other reports have been filed.
6. The Parties shall, after making notification and consulting with one another, take prompt corrective action to mitigate any harmful effect, risk, or damage involved with the breach or suspected breach.
7. The Parties agree to conduct an internal investigation of any reported breach or suspected breach and produce a written breach report within 10 working days of the incident. The internal investigation shall include:
 - a. Identification of each individual whose PII or PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the breach;
 - b. Brief description of the date of the breach and date of discovery (if known);
 - c. Description of the types of PII or PHI involved in the breach;
 - d. Steps, if any, individuals affected by the breach should take to protect themselves from potential harm resulting from the breach;
 - e. Data elements involved;
 - f. Description of the unauthorized persons known or reasonably believed to have improperly used or disclosed data received pursuant to this Agreement;
 - g. Description of where data received pursuant to this Agreement is believed to have been improperly transmitted, sent, or used;
 - h. Description of the probable cause of the breach; and
 - i. Description of the breaching Party's actions to mitigate the breach, and protect against future breaches including a detailed corrective active plan including measures that were taken to halt and/or contain the breach.

8. The Parties shall, as permitted by applicable State and federal laws, submit the breach report to one another's Privacy Officers and Information Security Officers, or persons responsible for privacy and information security.
9. Notification to Individuals
 - a. As required under State or federal law, NJDOH agrees to notify individuals whose information was subject to unauthorized access, use, or dissemination due to the breach of NJDOH data received pursuant to this Agreement.
 - b. For breaches of NJDOH data received pursuant to this Agreement due to the conduct of NJDOH, NJDOH shall be solely responsible for notifying individuals and the costs associated with such notifications.
 - c. For breaches of NJDOH data received pursuant to this Agreement that are due to the negligence or intentional misconduct of DLPS, NJDLPS agrees to cooperate with NJDOH on making notifications as directed by NJDOH and be responsible to NJDOH for the costs of such notifications.
 - d. As required under State or federal law, NJDLPS agrees to notify individuals whose information was subject to unauthorized access, use, or dissemination due to the breach of NJDLPS data received pursuant to this Agreement.
 - e. For breaches of NJSP data received pursuant to this Agreement due to the conduct of NJSP, NJDLPS shall be solely responsible for notifying individuals and the costs associated with such notifications.
 - f. For breaches of NJSP data received pursuant to this Agreement that are due to the negligence or intentional misconduct of NJDOH, NJDOH agrees to cooperate with NJDLPS on making notifications as directed by NJSP and be responsible to NJSP for the costs of such notifications.
 - g. If there is any question as to which Party is responsible for the breach, the Party whose data was breached shall issue a notice but the Parties shall subsequently determine responsibility for purposes of allocating the costs of such notices.

VIII. COMPLIANCE BY PARTY CONTRACTORS AND AGENTS

The Parties shall require that their respective contractors and agents, and, in the case of NJDLPS only, authorized law enforcement partners, who are provided with access to data received pursuant to this Agreement shall comply with the terms of this Agreement applicable to NJDLPS and be subject to the same privacy and

security safeguards obligated to the Party receiving data and as contained in this Agreement. The Parties further agree to incorporate, when applicable, the relevant privacy and security safeguards of this Agreement into subcontracts or subawards to their respective contractors, subcontractors, and agents.

IX. REQUESTS FOR INFORMATION

Court orders, including discovery requests, or freedom of information and open public records requests, including the New Jersey Common Law Right to Know and New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq., seeking information or documents regarding the data shared pursuant to this Agreement, shall be responded to and fulfilled by the Party that owns and maintains the data or record. A Party receiving a request or demand for information or data maintained by the other Party shall notify that Party in writing immediately after receiving the request.

X. COSTS

This Agreement is not an obligation or commitment of funds, nor a basis for a transfer of funds. Unless otherwise stated in this Agreement or separately agreed to in writing, each Party shall bear its own costs in relation to this Agreement. Notwithstanding any agreements relating to costs, expenditures by the Parties will be subject to their respective budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies an appropriation of funds for such expenditures.

XI. EFFECT ON OTHER AUTHORITIES

Nothing in this Agreement is intended to restrict the authority of any Party to act as permitted by law, or to restrict any Party from administering or enforcing any law.

XII. NO PRIVATE RIGHTS CREATED

This Agreement does not create any right or benefit, substantive or procedural, enforceable in law or in equity, against the State of New Jersey, or against any department, agency, officer, employee of the State of New Jersey, or against any Party to this Agreement, agency, or any other person.

XIII. NO THIRD-PARTY BENEFICIARIES

Neither Party intends to create in any other individual or entity the status of third-party beneficiary and this Agreement shall not be construed so as to create such status. The rights, duties, and obligations contained in this Agreement shall operate only between the Parties, and shall inure solely to their benefit. The provisions of this Agreement are intended only to assist the Parties in determining

and performing their obligations under this Agreement. The Parties agree that this Agreement shall not be enforceable as a matter of law or equity in any court or dispute resolution forum. Additionally, the parties agree that the conditions of this Agreement are not binding, and the sole remedy for non-performance under this Agreement shall be termination with no damages or penalty available to any party.

XIV. INDEMNIFICATION

The Parties agree, subject to any limitations imposed by law, rule, or regulation, to be responsible for the acts or omissions of their respective officials, employees, or agents and to cooperate in good faith to resolve any claims between the Parties promptly and, whenever appropriate, without litigation. For all such claims, each Party's point of contact will, within five business days of receipt, provide one another's designated legal representatives copies of any documents memorializing such claims.

XV. PERSONNEL NOT CONSIDERED STATE EMPLOYEES

Non-State employees performing services in connection with this Agreement shall not be considered employees of the State of New Jersey for any purpose, including but not limited to, defense and indemnification for liability claims, workers compensation, or unemployment.

XVI. NON-WAIVER

The failure by a Party to insist on performance of any term or condition or to exercise any right or privilege included in this Agreement shall not constitute a waiver of same unless explicitly denominated in writing as a waiver and shall not in the future waive any such term or condition or any right or privilege. No waiver by a Party of any breach of any term of this Agreement shall constitute a waiver of any subsequent breach or breaches of such term.

XVII. SEVERABILITY

If any of the terms and conditions of this Agreement are inconsistent with State or federal law, Party policy, or held by a court of competent jurisdiction to be invalid or unenforceable as a matter of law, the Parties shall confer and determine whether the remaining provisions of the Agreement shall continue in effect.

XVIII. APPLICABLE LAW

The terms of this Agreement shall be governed by the laws of the State of New Jersey.

XIX. TERM, TERMINATION, AND EXTENSION

- A. This Agreement is effective immediately upon the signature of both Parties and shall expire three years after its effective date.
- B. Any Party may terminate this Agreement for any reason or no reason by providing 30 days' written notice to the other Party.
- C. This Agreement also may be terminated immediately, upon written notice, should governing State or federal laws or regulations render performance hereunder illegal, impracticable, or impossible.
- D. The Parties agree that they may mutually agree to extend this Agreement for an additional period not to exceed two years, and if so shall confirm this in a signed writing attached to the Agreement as Attachment 4.

XX. DISPUTE RESOLUTION

For disputes related to this Agreement, including those concerning the data shared between the Parties, the Parties agree to first confer to resolve the dispute through the individuals who have day-to-day oversight of the responsibilities outlined in this Agreement. In the event that the Parties are unable to resolve the dispute through good faith efforts, the Parties agree to resolve the dispute through their respective responsible officials, or their designees, as identified in Section III(D).

XXI. ENTIRE AGREEMENT

This Agreement, including any amendments and attachments contained within it, represents the entire understanding and agreement between the Parties and supersedes all prior agreements and understandings between the Parties. Unless otherwise described in this Agreement, no amendment or modification of this Agreement shall be effective unless in writing and signed by both Parties.

SIGNATURE PAGE FOLLOWS

THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK

DATA USE AGREEMENT

BETWEEN

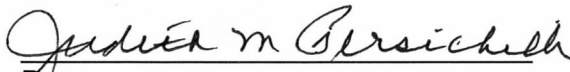
**THE STATE OF NEW JERSEY
DEPARTMENT OF HEALTH**

AND

**THE STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC SAFETY**

Now, therefore, in consideration of the mutual promises and undertakings contained herein, the Parties hereto consent to the provisions of this Agreement.

**Judith M. Persichilli, Commissioner
New Jersey Department of Health**

 Date: 6/1/23
By:
Title:

**Matthew J. Platkin, Attorney General
New Jersey Department of Law and Public Safety**



By: Matthew J. Platkin
Title: Attorney General

Date: May 31, 2023