



AIRA
AMERICAN IMMUNIZATION
REGISTRY ASSOCIATION

Example Policy Documents

IIS Community Policy Survey

July 22, 2019

Background

Policies and jurisdictional policy variation continue to strongly influence IIS functionality and interoperability. The American Immunization Registry Association (AIRA), in partnership with the Network for Public Health Law, performed several policy related projects in 2019 that will help to increase policy knowledge while supporting favorable policy decisions across the IIS community.

An AIRA Discovery session webinar was held on July 22, 2019 exploring considerations when developing IIS policy documents. The content for this webinar was developed through a community-wide questionnaire, key informant interviews with individuals from several IIS programs, and research of policy examples from the community to explore the strengths and considerations of various policy documents to support data use. Over 50 jurisdictions responded to the community questionnaire that focused on IIS policies or other terms and documents that govern data use. Several jurisdictions shared example policy documents they believe would serve as good examples to other jurisdictions. These examples are included in the following pages.

Please note that these examples were shared voluntarily from across the community and have been collected and reshared as examples only. Neither AIRA nor AIRA's legal counsel have reviewed or endorsed these policies or their content.

Examples

- Vendor Data Sharing Agreement, Alabama Department of Public Health submitted by Cindy Lesinger
 - Memorandum of Agreement, State of California Department of Public Health submitted by Steve Nickell
 - Health Plans Authorized Site Agreement, Iowa Immunization Registry Information System submitted by Kim Tichy
 - Memorandum of Agreement, Montana Department of Public Health and Human Services submitted by Michelle Funchess
 - HL7 Data sharing Agreement, Nevada WebIZ submitted by Amanda (Mandy) Harris
 - Data Security and Confidentiality Policy, New York City Department of Health and Mental Hygiene submitted by Amy Metroka
 - Data Sharing between Internal City Agencies, Philadelphia department of Public Health submitted by Aras Islam
 - Collaborative Agreement, Puerto Rico submitted by Veronica Rodriguez
-



**Alabama Department of Public Health
Immunization Division
Vendor Data Sharing Agreement**

THIS ELECTRONIC DATA SHARING AGREEMENT (“Agreement”) is made and entered into effective as of the date listed below, by and between ALABAMA DEPARTMENT OF PUBLIC HEALTH, an Alabama public health authority (hereinafter “**ADPH**”), and the Electronic Health Record (EHR) Vendor _____ (hereinafter “**TRADING PARTNER**”) to enable TRADING PARTNER’s applicable healthcare provider customers (each, a “**Healthcare Provider**”) to share immunization data between it and ADPH related to Healthcare Providers’ Alabama members in accordance with ADPH’s public health oversight authority as allowed by the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR 164.512(b).

WHEREAS, TRADING PARTNER maintains electronic information on Healthcare Provider’s patients receiving services at Healthcare Providers’ site(s); and

WHEREAS, ADPH maintains information on its Electronic Registries, which are statewide, centralized computerized database(s) created, owned, and maintained by ADPH and which contain information consisting of identifying, locating, and site data about former or current Alabama residents (hereinafter referred to as the “**ImmPRINT**”); and

WHEREAS, pursuant to Section 22-11B-1, et seq. Code of Alabama 1975, and Alabama Administrative Code Chapter 420-6-2.03, Health care providers shall provide immunization data about an individual upon the request of an immunization data user, by electronic means and in a timely manner. TRADING PARTNER will build an interface to enable Healthcare Providers to share information concerning the site status of patients receiving services at a Healthcare Provider’s site with ImmPRINT; and

WHEREAS, TRADING PARTNER will build the interface to share Healthcare Provider’s information between the Healthcare Provider and ImmPRINT, which is designed to provide information that identifies an individual’s site status, thereby promoting the proper information of individuals and the proper functioning of site programs.

NOW, THEREFORE, in consideration of the mutual covenants and promises herein contained the receipt and adequacy of which are hereby acknowledged by each party, the parties agree as follows:

Section 1. Definitions.

(a) “**Protected Health Information**” (PHI) shall be defined as individually identifiable health information transmitted or maintained in any form or medium including electronic media by 45 C.F.R. §160.103.



(b) “**Site Data**” refers to the date and/or type of site treatment received, including immunization information consisting of identifying, locating, and immunization data about former or current Alabama residents.

(c) “**Site Data User**” includes any individual or health care entity which is permitted to legitimately access Site Data in accordance with state or federal law, including TRADING PARTNER on behalf of its Healthcare Provider customers.

Section 2. Obligations of TRADING PARTNER. TRADING PARTNER is an EHR vendor for its health care entity clients in the United States and agrees to the following:

(a) **Data Exchange.** TRADING PARTNER will build an interface to enable Healthcare Providers to provide data about all immunization patients seen by such Healthcare Providers that indicates the vaccine type(s) and date(s) of vaccines administered, and historical date(s). TRADING PARTNER will enable Healthcare Providers to provide Site Data in a timely manner and from that facilitates achieving the appropriate site vaccines of a particular individual. TRADING PARTNER will not refuse or delay the exchange of Site Data by a Healthcare Provider to ImmPRINT.

Both parties agree to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality and integrity of the data and to prevent unauthorized use or access to it in accordance with the HIPAA Security Rule.

(b) **Merger and Acquisition.** TRADING PARTNER agrees to notify ADPH by email after 30 days of a merger, buyout or acquisition of TRADING PARTNER to ensure a minimum gap in connectivity. TRADING PARTNER shall submit the list of Alabama Healthcare Providers affected by the merger, buyout or acquisition with the notification.

(c) **Use of the ImmPRINT.** TRADING PARTNER agrees to complete the onboarding based on the ImmPRINT Onboarding Roadmap, HL7 Master Guide. In the event ADPH makes any change to the ImmPRINT Onboarding Roadmap, HL7 Master Guide, then ADPH will provide written notice to TRADING PARTNER of any such change at least sixty (60) days prior to the date that TRADING PARTNER is required to comply with such change. TRADING PARTNER will provide to ADPH a list of production, pilot production, and HL7/MU test sites. TRADING PARTNER will enroll and use the ImmPRINT to access and exchange Site Data. Only authorized users will be allowed access to the ImmPRINT through user accounts. Please see the Terms of Use for the ImmPRINT at <https://siis.state.al.us/ImmPRINT/User/MOU.aspx> for further details.

Section 3. Obligations of ADPH. ADPH agrees to provide to TRADING PARTNER electronic access to the ImmPRINT via TRADING PARTNER’S operated computer systems.

Section 4. Termination. Either party may terminate this Agreement upon thirty (30) days prior written notice to the other party. This will disable all security and site information, blocking future data transmissions from this TRADING PARTNER.



In the event that either party violates a material term of this agreement, the other party has the right to immediate termination of this agreement by providing notice to the breaching party.

Section 5. Independent Contractor Relationship. It is expressly acknowledged between the parties that each party is performing its obligations and duties under this Agreement as an “independent contractor” and nothing in this Agreement is intended nor shall be construed to create an employer/employee, master/servant, principal/agent, or a joint venture relationship.

Neither party, including such party’s employees, representatives, agents, attorneys, servants, successors or assigns shall have any right or authority to act on behalf of or to bind the other party in any manner whatsoever. The provisions of this Section shall survive the expiration or termination of this Agreement.

Section 6. Agent and Subcontractor Compliance. TRADING PARTNER shall ensure that any of its agents and subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which TRADING PARTNER receives from ADPH, agree to the restrictions and conditions which apply to the TRADING PARTNER hereunder regarding the privacy and security of such PHI. Failure to ensure that downstream contracts, subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement. TRADING PARTNER shall be solely responsible for all acts and omissions of TRADING PARTNER’s agents and subcontractors in their performance hereunder.

Section 7. Confidential Information. ADPH acknowledges and agrees that information shared pursuant to this Agreement is PHI and that ADPH will not use or disclose PHI exchanged pursuant to this Agreement other than as permitted by the applicable Healthcare Provider in an agreement between such Healthcare Provider and ADPH or as permitted by 45 C.F.R. §164.512(b)(1)(i), which provides that a covered entity may disclose PHI without prior authorization to a public health authority authorized to collect or receive such PHI for purposes of preventing or controlling disease. Further, it is the understanding of the parties that information obtained pursuant to the ImmPRINT is confidential, and thus, ADPH restricts other Site Data Users’ access to the ImmPRINT and provides Site Data only when there is a legitimate and professional need to know. ADPH further agrees that, when a Site Data User accesses the ImmPRINT, the only locating data accessible will be such data submitted by that Site Data User.

TRADING PARTNER agrees that the information in ImmPRINT is confidential and thus will only access it and provide it when there is a legitimate need to know as documented in this agreement or otherwise required by law.

Section 8. General.

(a) **Assignment.** This Agreement may not be assigned by either party, whether voluntarily or by operation of law, except to any successor to its business by merger, acquisition, consolidation or sale of assets, or to any entity controlling, controlled by or under common control with the assigning party. Subject to such limitation on assignment, the provisions of this



Agreement shall be binding upon and inure to the benefit of TRADING PARTNER and ADPH and their respective heirs, personal representatives, successors and assigns.

(b) **Notices.** All legal notices, requests, demands and communications required or permitted under this Agreement shall be in writing and shall be sent by traceable nationwide parcel delivery service or sent by certified United States mail. All other notices, requests, demands and communications required or permitted under this Agreement shall be in writing and shall be deemed to have been given by encrypted email. Proper notice will be deemed given 7 days after the date of mailing, and other notice will be deemed made when received.

If notice goes to TRADING PARTNER:

Organization Name:

Address

City, State, Zip

Attn:

Email:

If notice goes to ADPH:

ADPH/IMM

P.O. Box 303017

Montgomery, AL 36103-3017

Or

imprint@adph.state.al.us

With a copy to ADPH Attorney:

brian.hale@adph.state.al.us

or such addresses as TRADING PARTNER or ADPH may from time to time furnish in writing to the other pursuant to this Section.

(c) **No Waiver.** The waiver by either party of a breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of a subsequent breach of the same or other provision thereof.

(d) **Compliance with Laws.** The parties acknowledge and agree that none of the benefits granted to either party hereunder is conditioned upon any requirement that such make referrals to, be in a position to make or influence referrals to, or otherwise generate business for the other party.

(e) **Governing Law.** This Agreement shall be interpreted, construed and enforced according to the laws of the State of Alabama.

(f) **Entire Agreement.** This Agreement constitutes the entire Agreement of the parties hereto, and supersedes all prior agreements, oral or written, and all other commitments between the parties relating to the subject matter of this Agreement.



(g) **Force Majeure.** Neither party shall be liable to the other for failure to perform any of the services required herein in the event of strikes, lockouts, calamities, acts of God, unavailability of supplies or other events over which the affected party has no control, for so long as such event continues and for a reasonable period of time thereafter.

(h) **No Third Party Beneficiaries.** This Agreement is entered into for the sole benefit of the parties hereto. Nothing contained in this Agreement or in the parties' course of dealings shall be construed as conferring any third party beneficiary status on any person or entity who is not a party to this Agreement.

(i) **Amendments.** Any amendments must be in writing and signed by both parties in order to be binding.

(j) **Breaches.** Each party agrees to be liable for activity committed by their own workforce that creates a breach of protected health information. Should a breach of protected health information occur, the responsible party will adhere to breach notification requirements referenced in HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

IN WITNESS WHEREOF, ADPH and TRADING PARTNER have caused this Agreement to be executed by their duly authorized officers as of the ____ day of _____, 20____.

TRADING PARTNER

Signature: _____
Print Name: _____
Title: _____
Date: _____
Email: _____
Phone Number: _____
Address: _____

ALABAMA DEPARTMENT OF PUBLIC HEALTH

_____ Date: _____
Immunization Division Director



MEMORANDUM OF AGREEMENT

Parties

This Memorandum of Agreement (MOA) is made between the County of San Diego (County) by and through its Health and Human Services Agency (HHSA) and State of California Department of Public Health (State or CDPH). The parties to this MOA may be referred to herein collectively as the "parties" or individually as a "party".

Recitals

WHEREAS, the San Diego Immunization Registry (SDIR) is under the Public Health Authority of the County of San Diego, Health and Human Services Agency.

WHEREAS, the California Immunization Registry (CAIR2) is under the Public Health Authority of the State of California Department of Public Health.

WHEREAS, SDIR and CAIR2 are population-based electronic information systems providing exchange of patient demographic and immunization status among authorized participating organizations.

WHEREAS, a systematic exchange of patient and vaccine records between SDIR and CAIR2 systems will increase the effectiveness of both registry systems and benefit California and San Diego health services.

WHEREAS, SDIR and CAIR2 operate under the California Health & Safety Code which establishes registry operations including provisions to disclose registry information to each other as needed, as stipulated in subdivision (c) of section 120440 of the Health and Safety Code.

WHEREAS, the County using SDIR, and CDPH using CAIR2, agree to routinely exchange patient and immunization records as defined herein.

WHEREAS, the County and CDPH agree to limit their use of and protect the Protected Data according to the terms and conditions of this Agreement, and applicable state and federal law, as may be amended from time to time.

THEREFORE, in consideration of the foregoing recitals and the mutual covenants and promises set forth below, and for other good and valuable consideration, receipt of which is hereby acknowledged, the parties hereto agree as follows:

1. **Administration of MOA:** Each party identifies the following individual to serve as the authorized administrative representative for that party. Any party may change its administrative representative by notifying the other party in writing of such change. Any such change will become effective upon the receipt of such notice by the other party to this MOA. Notice of the authorized representative shall be sent to each party as follows:

<u>County</u>	<u>State</u>
Jeffrey Johnson Chief, Epidemiology & Immunization Services Branch Public Health Services Health & Human Services Agency 3851 Rosecrans St., Suite 704 San Diego, CA 92110 Phone: (619) 692-5633 Fax: (619) 692-6619 Email: Jeffrey.Johnson@sdcounty.ca.gov	James Watt, MD MPH Chief, Division of Communicable Disease Control, Center for Infectious Diseases California Department of Public Health 850 Marina Bay Parkway Richmond, CA 94804 Phone: 510-620-3784 Cell: 202-834-5988 Email: james.watt@cdph.ca.gov

2. Parties' Responsibilities

2.1. SDIR and CAIR2 will engage in data sharing activities as summarized in **Appendix A: SDIR-CAIR2 Data Sharing Plan**.

2.2. Obligations of CDPH and the County

- 2.2.1. **Use of Data Set:** CDPH and the County may use and disclose the Protected Data only as permitted under the terms of this MOA, or as permitted by law, but shall not otherwise use or disclose the Protected Data and shall ensure that directors, officers, employees, contractors, and agents do not use or disclose the Protected Data in any manner that would constitute a violation of this MOA.
- 2.2.2. **Minimum Necessary Information:** CDPH and the County agree that, to the extent that Protected Data is shared between CAIR2 and SDIR, as summarized in Section 2.1 Appendix A, only the minimum necessary Protected Data for the accomplishment of CAIR2 and SDIR's purpose will be shared.
- 2.2.3. **California Civil Code section 1798.29:** CDPH and the County recognize being subject to, and agree to comply with, the requirements of California Civil Code section 1798.29 with regard to Protected Data.
- 2.2.4. **Safeguards Against Misuse of Information:** CDPH and the County shall use appropriate safeguards to prevent use or disclosure of the Protected Data other than as permitted under this MOA.
- 2.2.5. **Information Security:** CDPH and the County shall comply with the information security standards outlined in **Appendix B: Data Security Standards**.
- 2.2.6. **Reporting of Disclosures of Protected Data:** CDPH and the County shall follow the procedure for initial reporting as outlined in Section 2.1, Appendix A.
- 2.2.7. **Agreements by Third Parties:** CDPH and the County shall obtain and maintain a confidentiality agreement with each agent or subcontractor that has, or will have access, to the Protected Data, which is received by or on behalf of CDPH or the County. Pursuant to which agreement such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to CDPH and the County pursuant to this MOA with respect to the Protected Data.

2.3. Definitions

2.3.1. "Confidential Information" means information that:

2.3.1.1. Does not meet the definition of "public records" set forth in California Government Code section 6252, subdivision (e), or is exempt from disclosure under any of the provisions of section 6250, et seq. of the California Government Code or any other applicable state or federal laws; or

2.3.1.2. Is required to be treated as confidential by state or federal law.

2.3.2. "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information.

2.3.3. "Protected Data" means:

2.3.3.1. Data in or from the SDIR or CAIR2 systems, or

2.3.3.2. Confidential Information

2.3.4. "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

2.4. Health Insurance Portability and Accountability Act (HIPAA):

2.4.1. CDPH CAIR2 System HIPAA Status: CDPH is a "hybrid entity" for purposes of applicability of the federal regulations entitled "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") (45 C.F.R. Parts 160, 162, and 164) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d - 1320d-8) (as amended by Subtitle D Privacy, of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5, 123 Stat. 265-66)). The CAIR2 system has not been designated by CDPH as, and is not, one of the HIPAA-covered "health care components" of CDPH. (45 C.F.R. § 164.504(c)(3)(iii).) The legal basis for this determination is as follows:

2.4.1.1. The CAIR2 system is not a component of CDPH that would meet the definition of a covered entity or business associate if it were a separate legal entity. (45 C.F.R. §§ 160.105(a)(2)(iii)(D); 160.103 (definition of "covered entity").) And

2.4.1.2. The HIPAA Privacy Rule creates a special rule for a subset of public health activities whereby HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." (45 C.F.R. § 60.203(c) [HITECH Act, § 13421, sub. (a)].)

2.4.2. Parties Are "Public Health Authorities": CDPH and the County are each a "public health authority" as that term is defined in the Privacy Rule. (45 C.F.R. §§ 164.501; 164.512(b)(1)(i).)

2.4.3. Protected Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of Protected Data may also be considered a disclosure or use of "Protected Health Information" (PHI) of an individual, as that term is defined in Section 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Protected Data disclosure and/or use by CDPH and the County, without the consent or authorization of the individual who is the subject of the PHI:

2.4.3.1. HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct

of public health surveillance, investigation, or intervention.” (45 C.F.R. § 60.203(c) [HITECH Act, § 13421, sub. (a)].)

- 2.4.3.2. A covered entity may disclose PHI to a “public health authority” carrying out public health activities authorized by law; (45 C.F.R. § 164.512(b).);
- 2.4.3.3. A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.” (Title 45 C.F.R. §§ 164.502 (a)(1)(vii), 164.512(a)(1).) and,
- 2.4.4. Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific Protected Data uses and disclosures.
- 2.4.5. No HIPAA Business Associate Agreement or Relationship Between CDPH and the County: This Agreement and the relationship it memorializes between CDPH and the County do not constitute a business associate agreement or business associate relationship pursuant to Title 45, CFR, Part 160.103 (definition of “business associate”). The basis for this determination is section 160.203(c) of Title 45 of the Code of Federal Regulations. (see [HITECH Act, § 13421, subdivision. (a)].) Accordingly, this Agreement is not intended to nor at any time shall result in or be interpreted or construed as to create a business associate relationship between CDPH and the County. By the execution of this Agreement, CDPH and the County expressly disclaim the existence of any business associate relationship.

- 3. **Indemnity:** [RESERVED]
- 4. **Insurance:** [RESERVED]
- 5. **Conformance with Rules and Regulations:** [RESERVED]
- 6. **Permits and Licenses:** [RESERVED]
- 7. **Governing Law:** This MOA shall be governed, interpreted, construed, and enforced in accordance with the laws of the State of California.
- 8. ***Live Well San Diego Vision:*** [RESERVED]
- 9. **Third Party Beneficiaries Excluded:** This MOA is intended solely for the benefit of County and State. Any benefit to any third party is incidental and does not confer on any third party to this MOA any rights whatsoever regarding the performance of this MOA. Any attempt to enforce provisions of this MOA by third parties is specifically prohibited.
- 10. **Amendments to MOA:** Any party may propose amendments to this MOA by providing written notice of such amendments to the other party. This MOA may only be amended by a written amendment signed by both parties.
- 11. **Severability:** If any terms or provisions of this MOA or the application thereof to any person or circumstance shall, to any extent, be held invalid or unenforceable, the remainder of this

MOA, or the application of such term and provision to persons or circumstances other than those as to which it is held invalid or unenforceable, shall not be affected thereby and every other term and provision of this MOA shall be valid and enforced to the maximum extent permitted by law.

12. **Full Agreement:** This MOA represents the full and entire agreement between the parties and supersedes any prior written or oral agreements that may have existed.
13. **Scope of MOA:** This MOA only applies to the program described herein and does not set forth any additional current or future obligations or agreements between the parties, except that the parties may by written amendment amend the scope of this MOA.
14. **Information Privacy and Security Provisions:** [RESERVED]
15. **Status of Provider:** [RESERVED]
16. **Term:** This MOA shall become effective on the date all of the parties have signed this MOA and be in force until June 30, 2021.
17. **Termination For Convenience.** State or County may, by written notice stating the extent and effective date, terminate this MOA for convenience in whole or in part, at any time.
18. **Counterparts:** This MOA may be executed in any number of separate counterparts, each of which shall be deemed an original but all of which when taken together shall constitute one and the same instrument.
19. **Confidentiality**
 - 19.1. Each party is individually responsible for abiding by the applicable laws and regulations pertaining to the data each has collected regarding clients.
 - 19.2. Nothing in this MOA shall relieve either party from abiding by relevant laws or regulations.
 - 19.3. All confidential client information obtained while on County property shall be treated in accordance with applicable federal and State law and County policy.

Remainder of this page is intentionally left blank

Appendix A: SDIR-CAIR2 Data Sharing Plan

1. Initialization.....	9
2. Interface SDIR → CAIR2	9
3. Interface CAIR2 → SDIR	9
4. Connection	10
5. Use Cases	10
5.1.1 Use Case 1.1.....	11
5.1.2 Sample HL7 Message from SDIR.....	11
5.1.3 Sample HL7 Message from CAIR.....	11
5.2 Use Case 1.2 (continuation of Use Case 1.1)	12
5.2.1 Sample HL7 Message from SDIR.....	12
5.2.2 Sample HL7 Message from CAIR.....	12
5.3 Use Case 1.3 (continuation of Use Cases 1.1 and 1.2)	13
5.3.1 Sample HL7 Message from CAIR.....	13
5.4 Use Case 2.1.....	13
5.4.1 Sample HL7 Message from SDIR.....	14
5.5 Use Case 2.2 (continuation of Use Case 2.1)	14
5.5.1 Sample HL7 Message from SDIR.....	14
5.5.2 Sample HL7 Message from CAIR.....	15

1. INITIALIZATION

1. SDIR will send demographic records and shots from all SDIR providers to CAIR2 in a flat-file format as specified by CAIR2.
 - a. A patient identifier and assigning authority pair will identify each demographic record.
 - b. Shots will also be associated with the patient identifier and assigning authority pair.
2. CAIR2 will match the records to its database.
3. CAIR2 will send back a download of its demographic and shot records that it has associated with the SDIR records in the same HL7 format that will be used in subsequent, nightly downloads (see further details below).
 - a. CAIR2 records will be identified by a CAIR2 assigned unique identifier (CAIR Patient ID).
 - b. CAIR2 will include the SDIR identifiers (patient ids and assigning authorities) of all SDIR records that it linked to CAIR2 record in the HL7 PID segment.
 - c. CAIR2 records not linked to any SDIR patient will not be sent.

2. INTERFACE SDIR → CAIR2

1. SDIR will send HL7 VXU messages in real time using the CDC SOAP WSDL to CAIR2 as records are updated in SDIR.
2. A patient identifier and assigning authority pair will be sent in the HL7 PID-3 field. The assigning authority will also be sent in the MSH-22 Responsible Sending Organization.
 - a. Assigning authorities will be sent as other patient IDs (OIDs)
3. VXUs will include all shots added, updated, or deleted during the transaction. I.e., when the record is saved in SDIR.
4. ADTs will be sent when a record is updated with no shot changes.
5. Merge, link and unlink and delete HL7 ADT records messages will be sent when records are merged, linked, unlinked or deleted at SDIR.
6. VXUs will adhere to the CDC HL7 Implementation Guide for Immunizations.

3. INTERFACE CAIR2 → SDIR

1. CAIR2 will send a batch of VXU messages to SDIR in batch HL7 messages each evening using the CDC SOAP WSDL.

2. The set of records returned will include all CAIR2 records created, updated or deleted since the last batch that are linked to at least one SDIR record.
3. Merges and links are included in the definition of “created, updated or deleted”. That is, changed CAIR2 records include any records changed by matching, including the match to an SDIR record or a non-SDIR record. HL7 messages will be sent when CAIR2 records are linked, unlinked, merged, or unmerged, whether to another CAIR2 record or to an SDIR record, if the set of records before or after the operation includes an SDIR record.
4. CAIR2 will send SDIR-only patients with two or more linked/merged patients back to SDIR, in addition to patients with at least one SDIR-CAIR2 link/merge. Messages will include all changes to patient records linked to SDIR patient records, including matching changes.
5. CAIR2 records not linked to any SDIR patient will not be sent.
6. The CAIR2 Patient ID will be sent in the first repetition of the HL7 PID-3 segment along with an ID type of ‘SR’.
7. The PID-3 segment will include all patient identifier and assigning authority pairs associated with the CAIR2 record, both SDIR and non-SDIR pairs. SDIR repetitions will have an ID type of ‘SDIRLink’. (This is the same format as in the initial upload)
8. The complete identifier list in the PID-3 segment is to enable SDIR to infer when links, unlinks, merges, unmerges and/or deletes may occur at CAIR2. As this solution is in lieu of the standard method of using ADTs to communicate matching changes, it needs to be prototyped in the early project phases.
9. VXUs will adhere to the CDC HL7 Implementation Guide for Immunizations.

4. CONNECTION

The CAIR2 interface will connect directly with SDIR using CDC’s SOAP WSDL.

5. USE CASES

In the use cases below, note that there are two possible interpretations to the question “Matching data found?”:

1. Matching *CAIR record* found?
2. Matching *record of any kind including an SDIR record* is found.

Returning only records that match to a CAIR2 record will reduce the number of records sent back. Returning all records will allow SDIR to determine whether CAIR2 has matched the records the same way SDIR matched them.

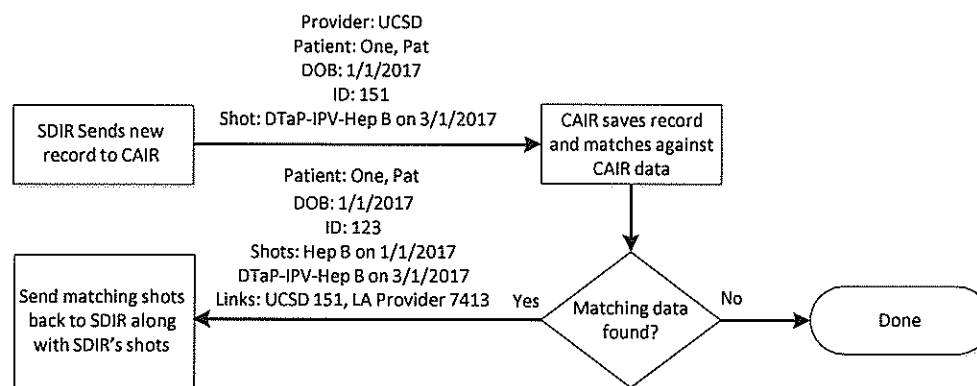
5.1.1 Use Case 1.1

New Patient seen by SDIR Provider: UCSD

One, Pat: DOB 1/1/2017

Shot: DTaP-IPV-Hep B 3/1/2017

Patient has a record in CAIR2 from a provider in LA



5.1.2 Sample HL7 Message from SDIR

```
MSH|^~\&|SDIR|SDIR|CAIR2|CAIR2|20170301101632||VXU^V04^VXU_V04|151|T|2.5.1|||ER|AL|||Z22^CDCPHI  
NVS|2.16.840.1.113883.4.514.4.4.1.296|CAIR|  
PID|1||151^^UCSD&2.16.840.1.113883.4.514.4.4.1.296&ISO^MR||One^Patient^A||20170101|M||2106-3|123  
ABC Street^#2^San Diego^CA^92122||6195551234||en|||||2186-5||N|  
PD1|||||||N|20170101|  
ORC|RE||2017072810151|  
RXA|0|1|20170301|20170301|110^DTaP-IPV-Hep B^CVX|999|||00^New  
Admin^NIP001||^2.16.840.1.113883.4.514.4.4.1.296|||ABC-123||MSD|
```

CAIR2 sends record back to SDIR with CAIR2 Patient ID and UCSD ID and echoes shot along with any matching CAIR2 shots.

5.1.3 Sample HL7 Message from CAIR2

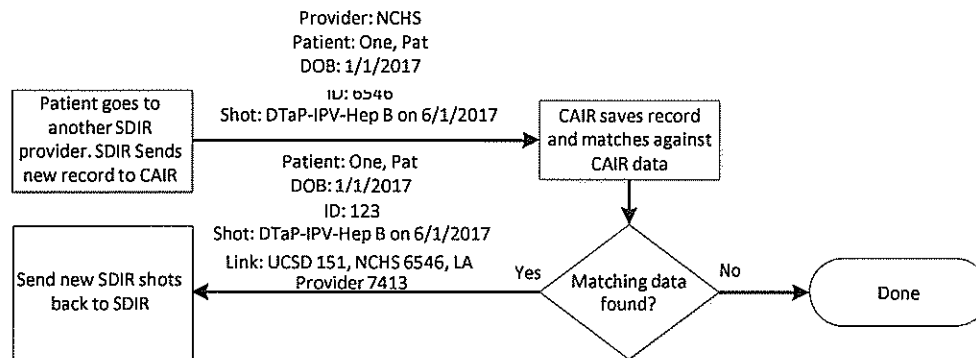
```
MSH|^~\&|CAIR2|CAIR2|SDIR|SDIR|20170301231632||VXU^V04^VXU_V04|  
2017072810151|T|2.5.1|||ER|AL|||Z22^CDCPHINVS|CAIR|SDIR|  
PID|1||123^^CAIR^SR~151^^UCSD&2.16.840.1.113883.4.514.4.4.1.296&ISO^SDIRLink~7413^^LA  
Provider^SDIRLink||One^Patient^A||20170101|M||2106-3|123 ABC Street^#2^San  
Diego^CA^92122||6195551234||en|||||2186-5||N|  
PD1|||||||N|20170101|  
ORC|RE||987098|  
RXA|0|1|20170101|20170101|08^Hep B^CVX|999|||00^New Admin^NIP001||^LA Provider|||ABC-123||MSD|  
ORC|RE||987099|  
RXA|0|1|20170301|20170301|110^DTaP-IPV-Hep B^CVX|999|||01^Historical^NIP001||^UCSD|||ABC-  
123||MSD|
```

5.2 Use Case 1.2 (continuation of Use Case 1.1)

Same patient seen by SDIR Provider: North County Health Services (NCHS)

One, Pat: DOB 1/1/2017

Shot: DTaP-IPV-Hep B 6/1/2017



5.2.1 Sample HL7 Message from SDIR

```
MSH|^~\&|SDIR|SDIR|CAIR2|CAIR2|20170601101632||VXU^V04^VXU_V04|151|T|2.5.1|||ER|AL|||Z22^CDCPHI  
NVS|NCHS|CAIR|  
PID|1||6546^^^NCHS&2.16.840.1.113883.4.514.4.4.1.14&ISO^MR||One^Patient^A||20170101|M||2106-3|123  
ABCStreet^#2^SanDiego^CA^92122||6195551234||en|||||2186-5||N|  
PDI|||||||||N|20170101|  
ORC|RE||2017030110456|  
RXA|0|1|20170601|20170601|110^DTaP-IPV-Hep B^CVX|999|||00^New  
Admin^NIP001||^2.16.840.1.113883.4.514.4.4.1.14|||ABC-123||MSD|
```

CAIR2 sends record back to SDIR with existing CAIR2 Patient ID and both UCSD and NCHS IDs and echoes shot.

5.2.2 Sample HL7 Message from CAIR2

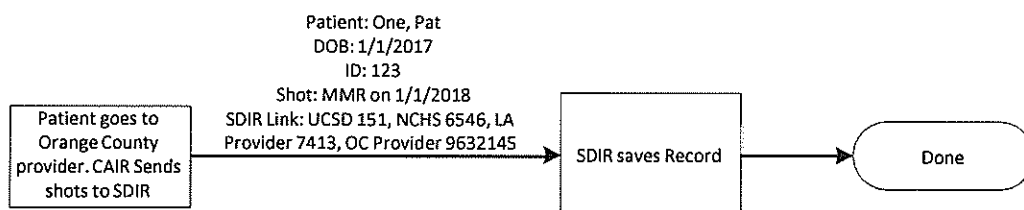
```
MSH|^~\&|CAIR2|CAIR2|SDIR|SDIR|20170302231632||VXU^V04^VXU_V04|  
2017072810151|T|2.5.1|||ER|AL|||Z22^CDCPHINVS|CAIR|SDIR|  
PID|1||123^^^CAIR^SR~151^^^UCSD&2.16.840.1.113883.4.514.4.4.1.296&ISO^SDIRLink~6546^^^NCHS&2.16.8  
40.1.113883.4.514.4.4.1.14&ISO^SDIRLink~7413^^^LA  
Provider^SDIRLink||One^Patient^A||20170101|M||2106-3|123 ABC Street^#2^San  
Diego^CA^92122||6195551234||en|||||2186-5||N|  
PDI|||||||||N|20170101|  
ORC|RE||987098|  
RXA|0|1|20170601|20170601|110^DTaP-IPV-Hep  
B^CVX|999|||01^Historical^NIP001||^2.16.840.1.113883.4.514.4.4.1.14|||ABC-123||MSD|
```

5.3 Use Case 1.3 (continuation of Use Cases 1.1 and 1.2)

Same patient seen by Orange County Provider

One, Pat: DOB 1/1/2017

Shot: MMR on 1/1/2018



CAIR2 sends shot to SDIR with existing CAIR2 Patient ID and both UCSD and NCHS IDs.

5.3.1 Sample HL7 Message from CAIR2

```
MSH|^~\&|CAIR2|CAIR2|SDIR|SDIR|20180102231632||VXU^V04^VXU_V04|
2017072810151|T|2.5.1|||ER|AL|||Z22^CDCPHINVS|CAIR|SDIR|
PID|1||123^^CAIR^SR~151^^UCSD&2.16.840.1.113883.4.514.4.4.1.296&ISO^SDIRLink~6546^^NCHS&2.16.8
40.1.113883.4.514.4.4.1.14&ISO^SDIRLink~9632145^^Orange County Provider^SDIRLink~7413^^LA
Provider^SDIRLink||One^Patient^A||20170101|M||2106-3|123 ABC Street^#2^San
Diego^CA^92122||6195551234||en|||||2186-5||N|
PD1|||||||||N|20170101|
ORC|RE||98465415|
RXA|0|1|20180101|20180101|03^MMR^CVX|999|||00^Administered^NIP001||^Orange County
Provider|||ABC-123||MSD|
```

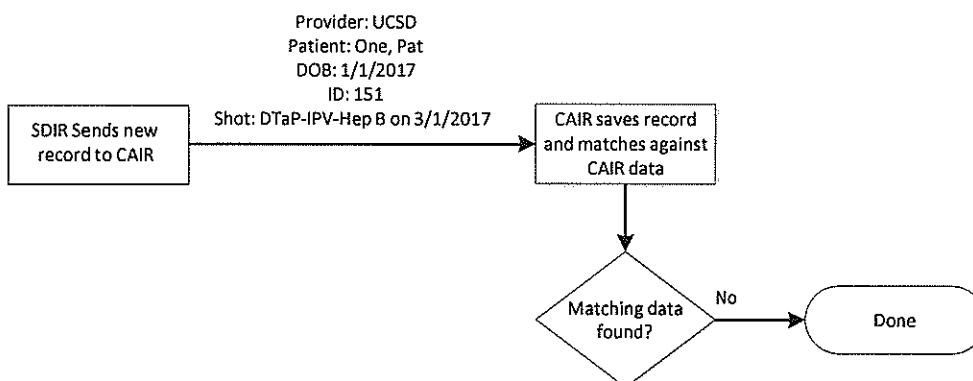
5.4 Use Case 2.1

New Patient seen by SDIR Provider: UCSD

One, Pat: DOB 1/1/2017

Shot: DTaP-IPV-Hep B 3/1/2017

Patient doesn't have a record in CAIR2



5.4.1 Sample HL7 Message from SDIR

```
MSH|^~\&|SDIR|SDIR|CAIR2|CAIR2|20170301101632||VXU^V04^VXU_V04|151|T|2.5.1|||ER|AL|||Z22^CDCPHI
NVS|2.16.840.1.113883.4.514.4.4.1.296|CAIR|
PID|1||151^^^UCSD&2.16.840.1.113883.4.514.4.4.1.296&ISO^MR||One^Patient^A||20170101|M||2106-3|123
ABC Street^#2^San Diego^CA^92122||6195551234||en|||||2186-5||N|
PD1|||||||||N|20170101|
ORC|RE||2017072810151|
RXA|0|1|20170301|20170301|110^DTaP-IPV-Hep B^CVX|999|||00^New
Admin^NIP001||^2.16.840.1.113883.4.514.4.4.1.296|||ABC-123||MSD|
```

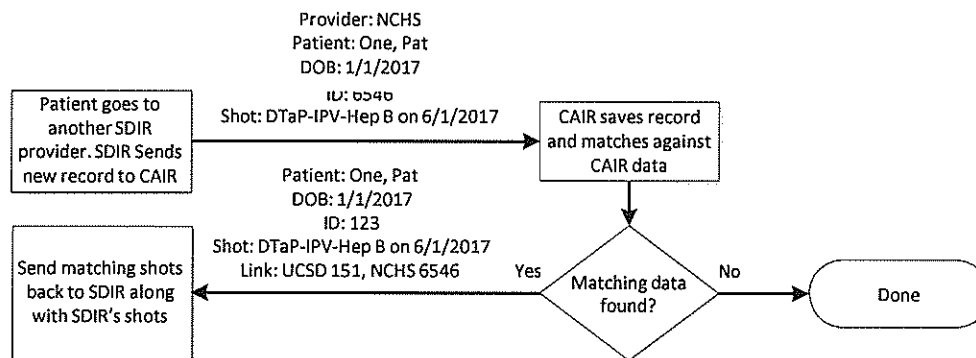
This is the only record in CAIR2 for this patient. Nothing is sent back to SDIR.

5.5 Use Case 2.2 (continuation of Use Case 2.1)

Same patient seen by SDIR Provider: North County Health Services (NCHS)

One, Pat: DOB 1/1/2017

Shot: DTaP-IPV-Hep B 6/1/2017



5.5.1 Sample HL7 Message from SDIR

```
MSH|^~\&|SDIR|SDIR|CAIR2|CAIR2|20170601101632||VXU^V04^VXU_V04|151|T|2.5.1|||ER|AL|||Z22^CDCPHI
NVS|NCHS|CAIR|
PID|1||6546^^^NCHS&2.16.840.1.113883.4.514.4.4.1.14&ISO^MR||One^Patient^A||20170101|M||2106-3|123
ABC Street^#2^San Diego^CA^92122||6195551234||en|||||2186-5||N|
PD1|||||||||N|20170101|
ORC|RE||2017030110456|
RXA|0|1|20170601|20170601|110^DTaP-IPV-Hep B^CVX|999|||00^New
Admin^NIP001||^2.16.840.1.113883.4.514.4.4.1.14|||ABC-123||MSD|
```

CAIR2 will send record back to SDIR with existing CAIR2 Patient ID and both UCSD and NCHS IDs. Note: CAIR2 could make a different matching decision than SDIR did.

5.5.2 Sample HL7 Message from CAIR2

```
MSH|^~\&|CAIR2|CAIR2|SDIR|SDIR|20170302231632||VXU^V04^VXU_V04|
2017072810151|T|2.5.1|||ER|AL|||Z22^CDCPHINVS|CAIR|SDIR|
PID|1||123^^^CAIR^SR~151^^^UCSD&2.16.840.1.113883.4.514.4.4.1.296&ISO^SDIRLink~6546^^^NCHS&2.16.8
40.1.113883.4.514.4.4.1.14&ISO^SDIRLink||One^Patient^A||20170101|M||2106-3|123 ABC Street^#2^San
Diego^CA^92122||6195551234||en|||2186-5||N|
PD1|||||||||N|20170101|
ORC|RE||987097|
RXA|0|1|20170301|20170301|110^DTaP-IPV-Hep
B^CVX|999|||01^Historical^NIP001||^2.16.840.1.113883.4.514.4.4.1.296|||ABC-123||MSD|
ORC|RE||987098|
RXA|0|1|20170601|20170601|110^DTaP-IPV-Hep
B^CVX|999|||01^Historical^NIP001||^2.16.840.1.113883.4.514.4.4.1.14|||ABC-123||MSD|
```

Appendix B

Data Security Standards

1. General Security Controls

- a. **Confidentiality Statement.** All CDPH and County workforce members that will have access to Protected Data must sign a confidentiality statement that includes at minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be physically or digitally signed by the workforce member prior to being given access to Protected Data. CDPH and the County shall retain each person's written confidentiality statement, whether in physical or electronic form, for inspection for a period of three (3) years following contract termination.
- b. **Workforce Member Assessment:** CDPH and the County, to the extent consistent with their governing statutes, regulations, existing contracts, rules and policies, must ensure that all workforce members that will have access to Protected Data have been assessed to assure that there is no indication that the workforce member may present a risk to the security or integrity of Protected Data. CDPH and the County shall retain each workforce member's assessment documentation, whether in physical or electronic format, for a period of three (3) years following contract termination.
- c. **Workstation/Laptop encryption.** All workstations and laptops that process and/or store Protected Data must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- d. **Server Security.** Servers containing unencrypted Protected Data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- e. **Minimum Necessary.** Only the minimum necessary amount of Protected Data required to perform necessary business functions may be copied, downloaded, or exported.
- f. **Removable media devices.** All electronic files that contain Protected Data must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, floppies, CD/DVD, smart devices, tapes, etc.). Protected Data must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128bit key or higher.
- g. **Antivirus software.** All workstations, laptops, and other systems that process and/or store Protected Data must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- h. **Patch Management.** All workstations, laptops, and other systems that process and/or store Protected Data must have operating system and security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

- i. **User IDs and Password Controls.** All users must be issued a unique user name for accessing Protected Data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared and must be at least eight characters; must be a non-dictionary word; must not be stored in readable format on the computer; must be changed every 60 days; must be changed if revealed or compromised and must be composed of characters from at least three of the following four groups from the standard keyboard:
 - Upper case letters (A-Z);
 - Lower case letters (a-z);
 - Arabic numerals (0-9); and
 - Non-alphanumeric characters (punctuation symbols).
- j. **Data Sanitization.** All Protected Data must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

2. System Security Controls

- a. **System Timeout.** The system must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- b. **Warning Banners.** All systems containing Protected Data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.
- c. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Protected Data, or which alters Protected Data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Protected Data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.
- d. **Access Controls.** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.
- e. **Transmission encryption.** All data transmissions of Protected Data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing Protected Data can be encrypted. This requirement pertains to any type of Protected Data in motion such as website access, file transfer, and e-mail.
- f. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting Protected Data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

- a. **System Security Review.** All systems processing and/or storing Protected Data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.
- b. **Log Reviews.** All systems processing and/or storing Protected Data must have a routine procedure in place to review system logs for unauthorized access.
- c. **Change Control.** All systems processing and/or storing Protected Data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of data.

4. Business Continuity/Disaster Recovery Controls

- a. **Disaster Recovery.** CDPH and the County must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Protected Data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.
- b. **Data Backup Plan.** CDPH and the County must have established documented procedures to back-up Protected Data to maintain retrievable exact copies of Protected Data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of back-up media, and the amount of time to restore Protected Data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. Paper Document Controls

- a. **Supervision of Data.** Protected Data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Protected Data in paper form shall not be left unattended at any time in vehicles, planes, trains, or any other modes of transportation and shall not be checked in baggage on commercial airplanes.
- b. **Escorting Visitors.** Visitors to areas where Protected Data is contained shall be escorted and Protected Data shall be kept out of sight while visitors are in the area.
- c. **Confidential Destruction.** Protected Data must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH Protected Data is no longer needed.

- d. **Removal of Data.** Protected Data must not be removed from the premises of CDPH except with express written permission of CDPH.
- e. **Faxing.** Faxes containing Protected Data shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.
- f. **Mailing.** Protected Data shall only be mailed using secure methods. Large volume mailings of Protected Data shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH-approved solution, such as a solution using a vendor product specified on the California Strategic Sourcing Initiative.



Immunization Registry Information System (IRIS)

Authorized Site Agreement – Health Plans

IRIS – Immunization Program
Lucas State Office Bldg., 5th Floor
321 E 12th Street
Des Moines, IA 50319-0075
Phone: (800)374-3958
Fax: (800)831-6292
<http://idph.iowa.gov/imm/tb/immunization>

Please complete and return to IRIS staff.

Name of Health Plan: _____
Physical Address: _____ City, State, Zip: _____
Mailing Address: _____ City, State, Zip: _____
Phone: _____ Fax: _____
Primary Contact Name: _____
Title: _____ Phone: _____ Email: _____
Authorized Representative (e.g. Managing Physician, CEO): _____
Title: _____ Phone: _____ Email: _____

Iowa's Immunization Registry Information System (IRIS) is a statewide database of immunization histories and health screening information maintained for the purposes of reminding patients of needed immunizations, facilitating vaccine inventory management, and providing organizations with the ability to search for and update patient records and to assess the need for immunizations and health screenings.

In order to participate in IRIS, this Health Plan agrees to the following:

1. Read and abide by the [IRIS Security and Confidentiality Policy](#), including procedures to safeguard user name(s) and password(s) against unauthorized use.
2. Use IRIS consistent with this agreement, the [IRIS Security and Confidentiality Policy](#) and Iowa law (Iowa Code § 22.7(2) and 641 IAC Chapter 7).
3. Collaborate with IRIS staff to submit any available historical immunization data on its enrollees in IRIS.
4. Utilize IRIS data to facilitate or conduct outreach to under-immunized health plan enrollees.
5. Actively promote participation in IRIS to health plan providers.
6. For the purposes of HEDIS reports and other performance measures, the health plan will work as needed with IRIS staff to submit a file, consistent with IRIS specifications, to IRIS for its health plan enrollees.
7. Comply with the purpose and permitted uses of the registry as detailed in 641 IAC 7.11.

Failure to abide by this agreement may result in immediate suspension or termination of access to IRIS and may result in other enforcement or action. By signing below, I agree to the above conditions and will abide in accordance with Iowa law:

Signature of Primary Contact: _____ Date: _____

Signature of Authorized Representative: _____ Date: _____

For Office Use Only

Date Received: _____ IRIS Org # Assigned: _____ Username Assigned: _____ Initials: _____

MEMORANDUM OF AGREEMENT



The Montana Department of Public Health and Human Services (DPHHS) and

(Organization)

hereby enters into the following Memorandum of Agreement (Agreement). The purpose of this Agreement is to identify each party's roles and responsibilities related to transmitting immunization information to and from Montana's Immunization Information System (IIS).

DPHHS agrees to:

- support and maintain the Montana Immunization Information System or IIS (hereinafter imMTrax);
- support and maintain the secured (encrypted) data communications mechanism for transmitting and receiving electronic immunization records;
- maintain staff availability during support hours: 8:00 AM to 5:00 PM, Monday through Friday (excluding state government holidays);
- maintain procedures to ensure the confidentiality, integrity, and availability of all data as required by applicable state and federal laws and regulations;
- maintain procedures to safeguard the integrity of imMTrax data in the event of a disaster;
- maintain and provide documentation related to HL7 specification and connection requirement;
- make every effort to maintain immunization data quality;
- notify organization through email, fax, or imMTrax announcements of events that impact imMTrax availability and use;
- provide organization with a single set of access credentials to be used to transmit and receive data via secured (encrypted) electronic communication facilities;
- validate the interoperability between the organization's system and imMTrax for submission of immunization data;
- validate the interoperability between the organization's system and imMTrax for real-time interfaces, if organization elects to make electronic queries;
- accept individual immunization record updates in either real-time or batch mode;
- accept real-time electronic queries from the organization to retrieve individual/patient immunization records if and when the organization elects to implement real-time interfaces with imMTrax;
- transmit resulting individual/patient immunization records to the organization based on real-time query parameters if and when the organization elects to implement real-time interfaces with imMTrax;

MEMORANDUM OF AGREEMENT



Organization agrees to:

- notify imMTrax staff of any change to designated organization contact person(s);
- immediately notify imMTrax staff of any intent to move to another electronic health record product;
- maintain procedures to safeguard individual electronic health records and systems to prevent improper access, use, or disclosure and to store immunization records in the event of a disaster. Such safeguards and procedures shall include training regarding security, confidentiality, and privacy issues for all staff involved in the transmission, access, use or disclosure of immunization data;
- maintain the confidentiality of all data as required by applicable state and federal laws; notify DPHHS as soon as reasonably possible of any significant breach, security incident, or improper access, use, or disclosure of imMTrax resulting from the conduct or omission of organization and/or its users, and take all necessary steps to mitigate any breach.
- limit access to imMTrax by the organization to only organization's users who must access and use for authorized treatment/care/data entry functions and only for appropriate patient care purposes for organization's clients;
- implement appropriate safeguards to prevent unauthorized access to electronic immunization records. This includes establishing automated system security practices that limits access to immunization records to only approved personnel;
- immediately remove an authorized user's access to electronic immunization records if the authorized user no longer qualifies as such;
- assure that any data obtained from imMTrax is only used to update organization's client health records maintained by the organization and not otherwise further used or disclosed;
- only use client individual immunization records for the purpose of recording and reporting individual health and medical records. Individual immunization records may be consolidated and used in aggregate form for assessment and for determining general health quality indicators;
- achieve connectivity to the data communications mechanism according to guidance found in the document *Connection Information*,
<http://dphhs.mt.gov/publichealth/imMTrax/DataExchange>;
- engage in a testing and validation process with DPHHS prior to sending electronic immunization data to imMTrax:
 - participate in validating the ability to transmit immunization records between the two parties;
 - identify method and provide extraction of immunization information from the organization's system to be used for data quality review;
 - implement modifications to internal practices that resolve data quality issues identified;
 - coordinate the implementation of software configurations that resolve data quality issues identified; and
 - satisfy DPHHS core elements and data quality standards established for immunization records when submitting immunization data;

MEMORANDUM OF AGREEMENT



- transmit individual electronic immunization records to imMTrax in either real-time or batch mode (no less than once per week);
- make every effort to rectify data quality issues reported by DPHHS;
- ensure data quality is sustained following initial validation at a level equal to the initial validation;
- maintain compliance with all HL7 message and quality standards;
- collect and include patient consent status in the transmission of immunization information to imMTrax. At DPHHS discretion, an organization whose EHR is not capable of collecting patient consent status may be permitted to transmit a status equivalent to *undetermined*; and
- coordinate any updates, modifications, additions, or removals of IIS codes as needed or upon notification.

Both parties (Parties) agree that:

- data transmission will be accomplished in accordance to DPHHS' document: *HL7 Implementation Guide*, <http://dphhs.mt.gov/publichealth/imMTrax/DataExchange>.

TERMINATION

Each Party shall have the right to immediately terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax exemption, federally funded health care program participation or licensure which: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a Party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally funded healthcare program, including without limitation the Medicare and Medicaid programs.

TERMINATION FOR CAUSE

Notwithstanding any other provision of this Agreement, any Party may terminate its participation in this Agreement if another Party has materially violated its responsibilities under this Agreement, unless the breaching Party provides satisfactory assurances to the non-breaching Party within ten (10) days or receiving notice of such material violation that reasonable steps are being taken to effect a cure, and in any event: (i) such cure will be completed no later than thirty (30) days from notice of such material violation; and (ii) the breaching Party has taken reasonable steps to prevent the recurrence of such material violation. TERM

This Agreement will be effective from the date of the last signature. Either Party may terminate this Agreement by giving thirty (30) days written notice to the other Part. This Agreement may only be amended in writing with the mutual consent of both parties.

The parties hereto have signed this Memorandum of Agreement on the dates indicated.

MEMORANDUM OF AGREEMENT



Organization Representative (CEO, Director, or Owner)

DPHHS Representative

Name (Signature)

Name (Signature)

Name (Typed or Printed)

Name (Typed or Printed)

Title

Title

Representing (organization name)

Representing

Date

Date



HL7 DATA SHARING AGREEMENT

Nevada State Immunization Program – Nevada WebIZ
4150 Technology Way, Suite 210
Carson City, NV 89706
PH: 775-684-5954 Fax: 775-687-7596



Nevada State Immunization Program
(hereinafter referred to as "NSIP")
and

Insert Provider Name
(hereinafter referred to as "**INSERT PROV ABBREV**")

This HL7 DATA SHARING AGREEMENT is hereby entered into between NSIP and **Insert Prov Abbrev**.

DESCRIPTION OF ELECTRONICALLY-STORED DATA TO BE PROVIDED

- Historical Immunization Data (*electronic documentation of immunizations administered by a provider other than **Insert Prov Abbrev** OR by **Insert Prov Abbrev** prior to their use of Nevada WebIZ*).
- Administered Immunization Data (*electronic documentation of immunizations administered by **Insert Prov Abbrev***).

SCOPE OF SERVICE

- ☒ **Insert Prov Abbrev** will submit to Nevada WebIZ all historical electronic immunization data (as defined above) in their possession to Nevada WebIZ. Historical immunization information submission is requested for the purpose of completing established immunization records in Nevada WebIZ.
- ☒ **Insert Prov Abbrev** will, on an ongoing basis, submit all administered immunization data to Nevada WebIZ (regardless of patient age).

TERMS OF AGREEMENT

This agreement shall commence upon the start of the project and will stay in affect as long as **Insert Prov Abbrev** is submitting immunization data to Nevada WebIZ. Data integrity is of the utmost importance and there are three facets of data quality to consider: formatting, accuracy, and completeness. **Insert Prov Abbrev** (or their IT support) shall be responsible for ensuring that all data is submitted in the correct format. **Insert Prov Abbrev** is also responsible for the accuracy and completeness of the data. **Insert Prov Abbrev** is responsible for the ongoing maintenance of these data quality facets along with correcting and resubmitting any incorrect data as long as **Insert Prov Abbrev** is submitting data to Nevada WebIZ.

EXPECTATIONS

- _____ **Insert Prov Abbrev** acknowledges that they (or their IT support) have working knowledge of the components, including any additional software and/or modifications to their electronic health record (EHR) software, necessary to establish an interface with Nevada WebIZ via web service.
- _____ **Insert Prov Abbrev** understands and recognizes that acknowledgement (ACK) messages sent via HL7 by Nevada WebIZ to **Insert Prov Abbrev** can and should be reviewed. **Insert Prov Abbrev** (or their IT support) will establish and implement an achievable protocol for monitoring these ACK messages on a regular basis, identifying errors, and for taking action to rectify identified errors.
- _____ **Insert Prov Abbrev** is responsible for verifying that the number of immunizations administered & documented in their EHR matches the number of immunization records that went into Nevada WebIZ. **Insert Prov Abbrev** will establish and implement an EHR/WebIZ Report Comparison process for verifying these numbers on a regular basis, identifying discrepancies, and taking action to rectify all discrepancies.

(Please initial)



HL7 DATA SHARING AGREEMENT

Nevada State Immunization Program – Nevada WebIZ
4150 Technology Way, Suite 210
Carson City, NV 89706
PH: 775-684-5954 Fax: 775-687-7596



UPDATING NEVADA WEBIZ RECORDS (VXU MESSAGE)

Method of Submission

_____ **Insert Prov Abbrev** will submit immunization data to Nevada WebIZ via web service. The frequency of submission will be **real-time, hourly, daily, or weekly.**
(Please initial)

QUERYING NEVADA WEBIZ RECORDS (QBP MESSAGE)

Though certain data quality measures are taken for aspects such as age appropriateness and timeliness, NSIP cannot guarantee the accuracy or validity of the data contained in the Nevada WebIZ database. Parties requesting data through a HL7 query (QBP) message assume liability for the validity of the data received in response to the query message.

Method of Retrieval (if applicable in the future)

_____ **Insert Prov Abbrev** will request immunization data from Nevada WebIZ via web service. The frequency of querying will be **real-time, hourly, daily, or weekly.**
(Please initial)

Nevada WebIZ is a confidential, population-based, computerized database used to record all immunization doses administered in Nevada and is maintained according to standards set by the Centers for Disease Control & Prevention.

Both Parties agree to protect the confidentiality of the data submitted to and stored in Nevada WebIZ, to use it only for purposes outlined by Nevada law and to not disclose the data to any third party.

The NSIP is HIPAA exempt because it does not provide direct medical services nor does it bill for medical services.

By signing this HL7 DATA SHARING AGREEMENT, both parties agree to the stipulations outlined in the agreement.

Insert Prov Abbrev will be asked to sign an HL7 Data Sharing Agreement every two years.

Nevada State Immunization Program

Insert Provider Name

Print Name

Print Name

Title

Title

Signature

Date

Signature

Date

Data Security and Confidentiality Policy
Division of Disease Control
New York City Department of Health and Mental Hygiene

Effective Date: May 12, 2017

Revision Date: May 12, 2017

I. SCOPE AND PURPOSE

This policy covers the scope of permissible use and requirements for maintaining the security of confidential information within the possession, custody, or control of the New York City Department of Health and Mental Hygiene (DOHMH) Division of Disease Control (the Division). This policy applies to all staff members.

For purposes of this policy:

- **Confidential information** is health information (e.g., disease status, testing and treatment information) and personal-identifying information related to a DOHMH patient, client, or individual made known to DOHMH pursuant to disease reporting, surveillance, or other public health activities, and acquired or maintained by the Division in any form or medium. This includes medical records, surveillance records and data, disease registry information, client information (e.g., case management files, files pertaining to participants in or recipients of Division services), and any other personal information obtained or received in the course of official duties. Personal-identifying information includes name, immigration status, address, telephone numbers, date of birth, social security number, workplace, medical records numbers, and any other information that can be used alone or in combination with reasonably accessible information to identify an individual. The type and sensitivity of personal-identifying information may vary by setting. For example, country of birth, age, and gender, taken together, could be used to identify an individual in certain settings.
- **Staff members** are all full-time, part-time, and temporary employees, contractors, consultants, interns, volunteers, and student workers at DOHMH working at or with the Division; staff members include individuals in other DOHMH divisions with access to confidential information acquired or maintained by the Division (e.g., Division of Informatics Information Technology and Telecommunications (DIITT) staff assisting with a Division project).

II. BACKGROUND

The mission of the Division is to safeguard the health of New Yorkers through the identification, surveillance, treatment, control, and prevention of infectious diseases.

In the course of these activities, staff members may need to access, use, and disseminate confidential information. The Division must ensure that confidential information is protected in accordance with

federal, New York State, and New York City laws, regulations, and guidelines. In addition, agreements between other government and public health authorities (e.g., New York State Department of Health; Centers for Disease Control and Prevention [CDC]) mandate that certain protections be in place. This policy shall be read in conjunction with, and as a supplement to, these materials. See Exhibit A, Laws and Regulations Governing Confidentiality, for links to relevant laws and regulations.

Several other DOHMH policies address the use and protection of confidential information and other DOHMH information, including the DOHMH Confidentiality Policy, Office and Technology Resources Acceptable Use Policy, Guidance Reducing the Risk of Inadvertent Disclosures for Tabular Data, DOHMH Data Transmission Policy, and Protocol for Entering Data Use Agreement (DUAs)/Non-Disclosure Agreements (NDAs) and Confidentiality Agreements. The most current versions of these policies can be found on the [Division Data Security and Confidentiality SharePoint site](#). Staff members are responsible for being familiar with these policies and any other policies and protocols currently in existence or later instituted by the Division or DOHMH related to the use and protection of confidential information and other DOHMH information. **At times this policy provides more strict requirements than those stated in agency policies; in such cases, the stricter requirements of this policy must be followed.**

Staff members should refer all questions regarding this policy to their bureau's Designated Confidentiality Coordinator (DCC), a staff member appointed by the Assistant Commissioner of each bureau to oversee the protection of confidential information. A list of current DCCs and their contact information can be found on the Division Data Security and Confidentiality SharePoint site. The DCCs assist in the development and implementation of policies and procedures at the bureau level and address inquiries regarding access to and use of confidential information, referring questions to the Chief Privacy Officer (CPO) in the Office of General Counsel (OGC) as necessary. The CPO has overall responsibility for preserving the security of confidential information for DOHMH. This policy was written under close advisement with the CPO and DCCs.

III. STAFF MEMBER TRAINING

All staff members must complete the Division online confidentiality training (available on HealthNet) prior to first accessing confidential information and annually thereafter. At the completion of the online training, each staff member must submit an electronic Confidentiality Acknowledgement attesting that they (1) have successfully completed the online training; (2) have read and understand this policy; and (3) agree to the requirements set forth in this policy. The bureau Assistant Commissioner or a designee is responsible for ensuring that staff members have up-to-date Confidentiality Acknowledgements.

Bureaus are responsible for ensuring that staff members receive updates related to this policy and other Division and DOHMH policies pertaining to the use, disclosure, and security of confidential information.

IV. ACCESS TO CONFIDENTIAL INFORMATION

Many staff members require regular access to confidential information in connection with their official duties, including patient care, laboratory testing, surveillance, case management, quality assurance, and research activities.

Absent the need for confidential information to carry out official duties and unless otherwise specified in this policy, staff members may not examine, read, delete, copy, alter, or remove confidential information. Thus, even where staff members are authorized to access confidential information, they should not access or view confidential information that is not necessary to conduct their official duties (e.g., information regarding a patient or case to which they are not assigned and to which access is not otherwise required to conduct official duties).

A. Access to Electronic Data Systems

Only staff members with a need to access surveillance data should be given access to applications and databases with confidential information (e.g., Maven, eHARS, ECLRS).

Staff members creating folders on the network drive that contain confidential information should work with DIITT to restrict folder access to staff members who require such information in the course of carrying out their official duties. Staff members must also ensure that access to confidential information posted on SharePoint is restricted to staff members who require access. Supervisors must request access to confidential information for their staff through the DIITT data systems administrator or other authorized individual; this may be done prior to a staff member beginning work. Supervisors are also responsible for promptly terminating access for a staff member who no longer requires access to confidential information.

Full access reviews of user and service accounts must be performed at least annually, with the bureau Assistant Commissioner or a designee signing off on the recertification of access lists. Credentials for access must be recertified in accordance with the application or database-specific schedule maintained by the Division and DIITT Security. Access to data systems with confidential information are subject to audit by the Division, DIITT Security, and other designated parties.

B. Remote Access to Confidential Information

By default, staff members should not have remote access to any data systems that contain confidential information. However, if access is necessary and allowed by written bureau protocol, a staff member's supervisor may request access from the DIITT data systems administrator. All remote access must be through DOHMH-approved means.

See Section VI.C. Security of Electronic Data and Documents for precautions that must be taken when remotely accessing confidential information.

V. USE AND DISCLOSURE OF CONFIDENTIAL INFORMATION

Disclosure is the release, transfer, provision of access to, or divulging of confidential information in any manner. Disclosure is allowed only where necessary as part of the staff member's official duties and only to persons or entities authorized to receive the information. Disclosures outside of those consistent with a staff member's routine duties must be approved by a supervisor or others (see Section V.D, Non-routine Disclosure of Confidential Information Outside of DOHMH).

Disclosures must only be made on a "need to know" basis, even to staff members in the same bureau, and only the minimum amount of information should be released. Persons receiving confidential information outside of DOHMH should be counseled not to re-disclose the information unless re-disclosure is necessary to treat the patient.

Staff members are not allowed to contact any person to whom confidential information pertains for reasons other than to perform official duties, and cannot discriminate, abuse, or take any adverse or other personal action against any person to whom confidential information pertains.

Staff members should ask their supervisor for guidance if unsure regarding the appropriate use or disclosure of confidential information *before* releasing such information. Supervisors should consult with their bureau DCC as necessary. Staff members should always err on the side of not releasing confidential information if there is any doubt as to whether release is appropriate.

Even after a staff member leaves employment or otherwise severs their relationship with the Division, the former staff member remains obligated to protect confidential information.

A. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law protecting the confidentiality of patient information and sets limitations on the disclosure of such information by "covered entities," namely, healthcare providers, healthcare clearinghouses, and health plans. HIPAA privacy and security rules apply to the following Division services:

1. Immunization Clinical Services
2. Sexual Health Clinical Services
3. Tuberculosis Clinical Services

[DOHMH's Statement Regarding Hybrid Entity Status Pursuant to HIPAA](#) provides an up-to-date list of DOHMH activities that are subject to HIPAA. Staff should consult with their bureau's DCC if they have questions regarding what activities are subject to HIPAA.

Under HIPAA, Protected Health Information (PHI)—individually identifiable information regarding a patient's past, present, or future medical conditions and care—may only be used and disclosed by covered entities with the patient's written authorization or where a few limited exceptions are met. One such exception is disclosure to a public health authority for public health purposes. More specifically, healthcare providers, such as DOHMH clinics, are permitted to disclose PHI without patient consent to a

public health authority authorized by law to receive such information, such as DOHMH, “for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.” HIPAA also allows disclosure of PHI “as required by law”—which includes state and local disease reporting requirements.

As such, HIPAA does not hinder provider reporting or cooperation with public health investigations, and confidential information obtained by healthcare providers, including DOHMH clinics, may be used by authorized DOHMH staff in conducting certain routine activities, including surveillance and case management. Additional information regarding patient identifiers protected by HIPAA can be found on the [Department of Health and Human Services website](#).

Public health activities performed by DOHMH that fall outside of the above-noted clinical services and related quality assurance and other activities are not subject to HIPAA. However, various New York State and New York City laws, rules, and regulations, this policy, and agreements between public health authorities (e.g., CDC) protect the confidentiality of such information.

B. Special Protection for Immigration Status

Pursuant to Mayoral Executive Order Nos. 34 and 41, staff members cannot inquire into an individual’s immigration status in performing case investigations, providing clinical services, or for any other purpose unless such information is necessary for the determination of a program, service, or benefit eligibility. Staff members may inquire regarding an individual’s country of birth, date of entry into the United States, and travel history if relevant to disease diagnosis or treatment, case management, contact investigation and other surveillance activities, or approved research. Further, immigration status, if known, must be kept strictly confidential and can only be disclosed by DOHMH in very limited circumstances (e.g., where the individual has given written consent; in connection with the investigation of potential terrorist activity). Assistant Commissioner approval is required for staff members to release information about the immigration status of an individual to anyone inside or outside of DOHMH.

C. Routine Disclosure of Confidential Information Outside of DOHMH

Some staff members may have to routinely disclose confidential information as part of their official duties. Organizations with which the Division routinely shares confidential information include:

- Patients, minor patients’ parents, legal guardians, and designated third-parties
- Patients’ healthcare providers and payers
- Organizations that provide services to patients, such as social service organizations, HIV/AIDS service organizations, and drug and alcohol rehabilitation centers
- Organizations that may have information about patients in their system, such as the New York City Human Resources Administration (HRA) and Department of Homeless Services (DHS)
- State, county, and municipal health departments and other government agencies
- Federal agencies, including the Department of Health and Human Services and CDC
- Health authorities in foreign countries

- Employers and persons in charge of schools, day cares, and other congregate settings, when the patient's disease may pose risk to others

Staff members may disclose confidential information to authorized persons as part of their official duties, including disease surveillance activities, case management, laboratory and clinic services, program evaluation, compliance monitoring, and contact and outbreak investigations.

New York State law delineates the limited circumstances under which confidential HIV-related information may be released. In general, authorized staff members may release HIV-related information only to the patient's current treating provider and state and local health departments when pertinent to treatment or for purposes of patient linkage and retention in care.

Following is additional information regarding certain types of routine disclosures.

1. Patient requests for medical records and information

Under HIPAA, a patient or legal guardian has the right to request his or her medical records from DOHMH clinics. Confidential information about the patient may be released to a third-party if the patient specifically authorizes it by signing an approved authorization form that indicates to whom the information may be released.

A general authorization is not sufficient to release HIV, drug and alcohol treatment, or mental health records; release of such records requires written consent specific to the type of information. Consent forms for release of HIV-related information must comply with Section 27-F of NYS Public Health Law; examples of acceptable consent forms can be found on the [New York State Department of Health website](#).

The Division cannot release records to a parent or legal guardian concerning the diagnosis or treatment of a sexually transmitted infections in, or the performance of an abortion on, a minor less than eighteen years of age without the consent of the minor patient. A healthcare provider may also deny access to medical information where the provider determines that the release of information is expected to cause harm to the patient or others, outweighing the patient or other requestor's right to access such information.

2. Release of confidential information for medical and billing purposes

Authorized staff members are allowed to release patient information, including test results, to authorized healthcare providers who are currently providing care to a patient where such information is pertinent to the patient's care. Patient consent for such disclosures is not needed but the disclosure must be documented in the patient's medical or disease registry record.

Patients at DOHMH clinics receive a notice of privacy detailing permissible disclosure, including sharing standard medical and billing information with third-party payers (e.g., insurance companies, Medicaid) based on HIPAA transaction rules. The Division can share a copy of the

billing encounter form with treatment recommendations regardless of whether the third-party payer makes a request.

Pursuant to HIPAA, clinic patients have a right to request information regarding disclosures made without their authorization for the six-year period preceding the request; however, disclosures made for treatment, payment, and other limited reasons outlined in HIPAA are excluded from this requirement.

3. *Communications with government entities*

The Division reports test results and cases to authorized federal, state, and local agencies in compliance with existing laws and regulations and, in some cases, agreements with those parties. Information may also be shared with a health authorities in foreign countries where, for example, an infectious patient leaves the country. Patient consent for such disclosures is not needed, but individual disclosures regarding specific patients must be documented in the patient's disease registry record.

4. *Contact investigations*

Confidential information may need to be shared with a patient's employer or the person in charge of a school, day care, nursing home, or other congregate setting if the patient's medical condition may have posed a risk to others. This generally occurs in the context of a contact investigation, where staff members need to identify individuals who may have been in contact with an infectious patient. Patient consent for such disclosures is not needed but all such disclosures must be documented in the patient's disease registry record.

D. Non-Routine Disclosure of Confidential Information Outside of DOHMH

Non-routine disclosures are those in which disclosures are not a part of daily operations. Non-routine disclosures generally require approval from a supervisor or other designated individual, who will consult with the bureau DCC and OGC as necessary.

The following are examples of non-routine disclosures:

- ***Subpoenas, court orders, Freedom of Information Law requests, and other legal orders/requests.*** All such documents must be promptly brought to the attention of the staff member's supervisor for forwarding to OGC.
- ***Medical emergencies.*** Confidential information may be released to medical personnel if necessary to treat the patient during a medical emergency; in such cases, it may not be possible to obtain supervisor approval prior to doing so.
- ***Research.*** Access to patient records and other confidential information may be allowed for research purposes. The research protocol must ensure that confidentiality will be maintained and the protocol must receive DOHMH Institutional Review Board (IRB) approval or a determination must be made that no IRB approval is needed. Abstracts for submission to scientific conferences or manuscripts for submission for publication must undergo bureau,

Division, and DOHMH clearance and meet standards for data dissemination. See DOHMH agency-wide Confidentiality Policy for more information on research protocols.

- **Audits.** Audits and evaluations by an outside agency or other entity may involve review of confidential information; such audits/evaluations are generally subject to an agreement with the outside entity that delineates scope and provides confidentiality protections. For audits conducted by DOHMH, persons conducting the audit who will have access to confidential information are considered staff members, as defined in this policy.

E. Release of Aggregate Data

Aggregate data is data compiled from individually-identifiable information and grouped in a manner to preclude the identification of individuals. The Division shares aggregate data with other DOHMH programs and city, state, and federal agencies routinely and upon request. Aggregate data are also routinely released to the public via the Division's surveillance summaries and other reports and the DOHMH website, including through EpiQuery. Aggregate data may also be released in response to a specific request by the media or other entity.

Aggregate data disseminated outside of DOHMH must be restricted to ensure that a combination of data elements that are not separately identifying cannot enable the identification or near-identification of an individual, for example, where the relevant population is too small. For further guidance, refer to DOHMH Guidance Reducing the Risk of Inadvertent Disclosures for Tabular Data.

Supervisor approval is required to release aggregate data outside of DOHMH if the data has not previously been published or made publically available.

F. Sharing Data Outside of DOHMH; Data Use Agreements

When sharing confidential information outside of DOHMH, a Data Use Agreement (DUA) may need to be executed between the Division and other entity. DUAs establish the type of confidential information to be shared, who will have access to it, limitations on use, and rules for dissemination. A DUA is not necessary (i) for routine disclosures, (ii) when sharing publicly-available data (e.g., data available on EpiQuery or released in annual reports), and (iii) for certain non-routine disclosures, such as data produced as required by law, in connection with audits, and in medical emergencies. A DUA should be executed in most other circumstances.

If a DUA is necessary, the staff member overseeing the data-sharing should utilize the DUA template, issued by OGC (available on Division Data Security and Confidentiality SharePoint site). If no changes are made to the template, approval from OGC is not necessary; any variations in language from the DUA template require approval from OGC by coordinating with the Chief Privacy Officer (CPO). See DOHMH Protocol for Entering Data Use Agreement (DUAs)/Non-Disclosure Agreements (NDAs) and Confidentiality Agreements.

In addition to the formal DUA process, each bureau should assess the efficacy of data requests received and whether, legal considerations aside, the proposed data-sharing is appropriate and in the best interests of DOHMH. Considerations include the reputation and type of entity being provided with the

data, the scope of the data requested, and intended use of the data (i.e., is the intended use something with which DOHMH should be associated).

When staff members are seeking data from a non-DOHMH entity, the entity may request that DOHMH sign a DUA. All such DUAs are subject to OGC approval. The staff member overseeing the project or a designee must coordinate with the CPO.

The Deputy Commissioner or a designee must sign the DUA on behalf of DOHMH. The individual signing on behalf of the other party must be able to bind that entity. This can be ascertained by the individual's title (e.g., President, Vice President, CEO) and confirming with the entity that the individual has signatory authority by reaching out to that entity's legal counsel or senior officers.

A copy of all executed DUAs (even if no changes were made to the OGC template) must be sent to the CPO by email. Where original (non-electronic) signatures are required for execution, the bureau is responsible for maintaining the original signed document. Corresponding cover letters and emails should also be maintained.

G. Sharing Data with Other DOHMH Programs

A DUA is not necessary or appropriate when sharing data between Division bureaus or with other DOHMH offices or divisions. Rather, the Division Data Request Form (available on the Division Data Security and Confidentiality SharePoint site) summarizing the information needed, timeframe, and intended use should be completed.

If the parties agree, the form need not be used for minor data requests. Also, the form may be bypassed in emergencies, such as urgent Commissioner of Health or City Hall requests and requests in connection with Incident Command System (ICS) activation, in which case ICS protocols should be followed.

All DOHMH personnel given access to confidential information are considered "staff members," as defined in this policy. The requestor must confirm that all staff members who will have access to the data have an up-to-date Confidentiality Acknowledgement (i.e., dated within the last year).

Use of the data by receiving program staff members should be in close consultation with the program supplying the data, and in all cases the receiving program must consult with the program supplying the data before disclosing it outside of the agency, including in published manuscripts or abstracts (even if only aggregate data is used).

H. Transmission of Confidential Information

Below are requirements for maintaining the security of confidential information disclosed through various means. The permissible use of each disclosure method varies by the information being disclosed, to whom the disclosure is made, and the staff member's official duties. Bureau protocols provide additional information regarding which staff members may use certain types of media, such as text messaging or fax, and under what circumstances particular media may be used. The below requirements are to be followed in conjunction with the DOHMH Data Transmission Policy and bureau protocols.

1. *In-person discussions*

Confidential information must not be discussed orally except to authorized persons with a need to know and in an appropriate confidential setting. When discussing confidential information at work stations, staff members must communicate with discretion to minimize the risk of exposing confidential information to persons who do not need to know. This includes speaking in a low tone and using non-identifying information if possible (e.g., stating “20-year-old male patient” instead of the patient’s name). Oral discussion of confidential information is prohibited in public places, including common areas of DOHMH buildings such as elevators and the lobby.

Staff members must take measures to avoid disclosure of confidential information to unauthorized persons. For example, staff members can ask a patient’s neighbor or family member about the patient’s whereabouts, but cannot divulge information about the patient’s health. Identifying oneself as DOHMH staff may be necessary to find a patient; however, staff members must not disclose their program or bureau affiliation or any confidential information.

2. *Telephone calls*

Release of confidential information over the telephone must comply with the following procedures:

- Do not mention a specific bureau, program, disease, or condition when answering your workstation or work mobile phone; leaving a voicemail message for patients/clients; or speaking with anyone other than the patient/client in attempts to contact the patient/client.
- Only call patients/clients at their workplace as a last resort.
- Verify the identity of callers, especially clinical staff calling about a patient, including by asking for a medical license number if necessary (patients and family members have called pretending to be the physician).

Specific inquiries:

- Staff members working in directly observed therapy (DOT) programs must follow-written bureau protocol for verifying the identity of the DOT participant.
- Staff members conducting expanded contact investigations may release confidential information over the phone to authorized individuals following written bureau protocol.
- Staff members speaking with managed care organizations (MCO) must verify callers using the MCO Designated Liaison Authorization List.
- Telephone reporting of laboratory test results by the Public Health Laboratory is not favored and is limited to non-business hours and non-routine inquiries, such as those attendant to an ICS activation or outbreak investigation. Such reports will be made only to DOHMH physicians and other authorized staff members associated with the case or investigation.

3. Text messages

Text messages may be sent to patients, clients, and individuals in connection with a case, contact, or outbreak investigations, as follows:

- Text messages may be sent only by staff members whose official duties include communicating with such individuals and only when authorized by written bureau protocol.
- The individual to whom the text is being sent must either give consent to receiving text messages from DOHMH or be given an opportunity to “opt out” of receiving text messages. If consent is not received prior to first communicating by text, the following text must appear in either the first or second message sent to the individual, and in every message thereafter until the individual consents to receiving text messages: “Reply ‘STOP’ to stop receiving text messages.”
- Text messages may only be sent using a DOHMH-issued mobile phone or email account.
- Text messages must never include any names or other identifiers (other than the telephone number used for texting) or mention a specific bureau, program, disease, or condition with the exception of general educational information about a disease or condition if permitted by written bureau protocol.
- Text messages can include administrative information (e.g., appointment reminders but without stating the type of clinic) and requests to call DOHMH.
- If an individual sends a text message to a staff member asking for clinical or other confidential information, the staff member must not disclose any such information and instead encourage the individual to call for additional information (or the staff member may affirmatively call the individual to discuss).
- If a text message from an individual includes confidential information (e.g., information indicating the disease or condition), the message must be deleted and the incident must be documented in the patient/client’s medical or disease registry record.

Text messaging between staff members or with partners/colleagues outside of DOHMH should be limited to non-confidential administrative functions and messages must not contain any confidential information.

4. Hardcopy mail

When mailing hardcopy documents containing confidential information is permitted by written bureau protocol, staff members must use envelopes marked “Confidential.” For correspondence with patients or program clients, envelopes must not contain any reference to a specific bureau, program, disease, or condition.

A medical record or disease registry number should be used instead of the patient’s name in corresponding with someone other than the patient, when possible. In correspondence copied (cc’d) to other individuals for administrative purposes, confidential information must be redacted unless necessary to accomplish the administrative function.

5. Email

Disease registry numbers and other DOHMH-assigned unique identifiers (preferable) or medical record numbers may be used in the body of an email; no other confidential information may be included in the body or subject line of an email. This holds true for both internal emails (intra-agency) and external emails (emails to third parties, including patients). General descriptions of patients (e.g., 32-year-old female with syphilis) may be included in the body of emails.

Following are the rules for sending emails (internal and external) with confidential information:

- Confidential information must be sent by way of password-protected attachment(s).
 - To password-protect a file, follow the step-by-step instructions for Microsoft Office documents (e.g., Word, Excel) and PDFs, found at Exhibit B. Documents in other formats (e.g., SAS output) should be exported to a Microsoft Office document.
 - Only Microsoft Office 2007 or later can be used to password-protect a file.
 - Passwords must be communicated orally by phone.
- In addition to password-protecting the file, the word “encrypt” with brackets must be typed at the beginning of the subject line of the email as follows: [ENCRYPT]. When responding to email chains, staff members should check to ensure that “[ENCRYPT]” has been preserved in the subject line.

If an incoming email includes confidential information and does not conform to the above standards:

- Promptly delete the email from the Inbox and Trash folders and instruct persons copied on the email to do the same.
- Instruct the sender not to transmit confidential information by email except in an encrypted attachment.
- Delete the confidential information from the email chain if forwarding or replying to the message.
- Record the incident in the patient/client’s medical or disease registry record.

6. Faxes

Use of faxes to transmit confidential information should be minimized. When faxing is necessary, only secure fax machines may be used. A secure fax machine is one dedicated solely to a work unit whose business routinely includes sending and receiving confidential information, such as surveillance units. The work unit is responsible for monitoring the fax machine to help ensure transmissions with confidential information are not accessible to persons not authorized to view confidential information, including by timely retrieving faxes during working hours.

When sending faxes with confidential information, staff members must use a standard fax cover sheet marked “Confidential” in large font and stating the sender’s name and contact information, recipient’s name and fax number, transmission date, the number of pages to be

faxed, instructions for return of information if inappropriately received, and a confidentiality disclaimer. Staff members must call the recipient just prior to transmitting the fax to help ensure prompt retrieval; staff members should verify the fax number and request that the recipient confirm receipt. Staff members must ask individuals sending faxes with confidential information to DOHMH to use an appropriate cover sheet and notify prior to sending.

VI. SECURITY OF DATA AND CONFIDENTIAL INFORMATION

A. Facility Security

Visitors to DOHMH non-clinic facilities require security clearance and should generally be accompanied at all times. Staff members must not permit anyone without a DOHMH identification card or time-limited entry pass issued by DOHMH Police to enter individual floors and other secure areas. Visitors should be instructed not to walk around the floors/building on their own.

Certain areas within a bureau's designated office space (e.g., surveillance units) have additional security access requirements. Access may be limited to bureau staff or even specific bureau staff members. Staff members must be careful to ensure that unauthorized persons do not enter these areas, including by making sure doors are closed and locked behind them.

B. Security of Paper Documents

The following precautions must be taken to maintain the security of paper documents with confidential information (e.g., patient records, case reports, field notes and logs):

- Do not leave such documents unattended on desks or out in the open when not in use. Such documents must be maintained in designated file cabinets or, when permitted by written bureau protocol, a staff member's locked desk drawer.
- Avoid photocopying and printing as much as possible. When printing, faxing, or copying such documents, retrieve promptly and shred when no longer needed. Do not leave a fax machine or printer until the job is complete.
- Where paper records have access logs, log when a record was accessed, removed, and returned.
- Do not remove such documents from a DOHMH premises without supervisor approval, unless permitted to do as part official duties and pursuant to written bureau protocol.

When removing documents with confidential information from a DOHMH premises, care must be exercised to ensure that materials remain secure, including by adhering the following rules:

- Materials must be kept with the staff member at all times (e.g., confidential information should not be left in cars), unless the Assistant Commissioner overseeing the program has established a written protocol approved by the CPO carving out an exception.
- Materials must be returned to their original location as soon as possible.
- Materials must be stored in a secure manner, ideally within an envelope marked "Confidential" and that includes a contact phone number on the front.

- Materials that must be brought home are to be secured in a safe place, out of sight, and separate from personal items.
- A supervisor must be immediately notified if materials are lost or stolen.

C. Security of Electronic Data and Documents

Staff members are responsible for maintaining the security of electronic data and documents at their individual and communal (e.g., conference room) workstations, including by adhering to the following requirements:

- Do not leave confidential information visible on a computer screen while workstations are unattended; screens can be locked using the Ctrl-Alt-Delete key combination or via the 'Start' menu in the lower left-hand corner of the desktop and should automatically time out when inactive.
- Log out of medical records and disease registry (e.g., Maven, eHARS) systems as soon as a work session is complete.
- Log out of conference room and other shared computers at the end of work sessions.
- Do not share individually-assigned network, registry, or other DOHMH systems passwords with anyone, and only access DOHMH systems using your assigned log-in ID and password.
- Do not enable web browsers or other software to save passwords to medical record, disease registry, and related systems (e.g., Maven, ECLRS, EDRI, eHARS); these passwords must be entered every time the staff member logs on to the secure system.
- All files containing confidential information must be stored on a DOHMH network drive (e.g., J, R, S drive) or SharePoint, and must never be stored on the computer desktop or hard drive.
 - Storage within a folder on a shared network drive (e.g., R or S drive) is permissible only if those who have access to the folder have reason and permission to access the confidential information; DIITT can create secure folders on the R or S drive that are accessible to only a limited set of users.
 - When posting on SharePoint, the person posting the documents is responsible for restricting user access to the site; do not post confidential information on a SharePoint site unless confident that user access has been appropriately restricted.
- Even where documents are properly stored on a network drive, whenever possible, a disease registry number or other record ID number should be used instead of patient names within documents to reduce the risk of inadvertent disclosure.

The following rules regarding remote access to confidential information must be followed:

- Remote access must be through DOHMH-approved means, such as DOHMH Remote Access (also known as virtual private network [VPN]), AirWatch, Outlook web access, and DOHMH-issued tablets, smart phones, and other devices.
- All tablets, smart phones, and other portable electronic devices used for DOHMH activities must be password-protected.

- Staff members must not connect to the internet via public WIFI, but use only private, password-protected networks or the cellular network to access the internet.
- Staff members remotely viewing confidential information must take precautions to ensure the environment is sufficiently private to prevent others from viewing the confidential information (e.g., ensure screens are not viewable by others).
- Confidential information must never be stored on any type of unencrypted portable electronic device (e.g., USB drive, external hard drive, DVD/CD), or on non-DOHMH devices, such as home computers and personal smart phones. Only DIITT-issued devices (e.g., Ironkey) may be used to store confidential data.
- Do not lend DOHMH-issued portable electronic devices (e.g., smart phones, tablets, thumb drives) to other staff members or anyone else.
- Immediately contact DIITT if a portable electronic device is lost or stolen, including your personal smart phone when used pursuant to the Bring Your Own Device program, so that all DOHMH accounts can be disabled.

D. Staff Member Departures

When a staff member ceases work with the bureau (or changes his or her job assignment and no longer requires access to confidential information), the staff member's supervisor or a designee must work with DIITT to ensure that the staff member's hard drive and DOHMH-issued portable electronic devices (e.g., tablets, smart phones) are irreversibly purged of all confidential information and that network access is terminated; an email should be sent to the DIIT person assigned to the task confirming this has been done. The supervisor or a designee must also ensure the staff member's work station is cleared of all hardcopy documents containing confidential information.

E. Records Retention and Destruction

Records retention is governed by the DOHMH Records Retention Schedule, issued by the NYC Department of Records & Information Services (DORIS). The DOHMH Records and Document Management Policy provides additional detail regarding the types of records that must be retained, where and for how long, and conditions and means of destruction. Records retention schedules are based on local, New York State, and federal requirements and defer to whichever is longer. Individual bureaus may also have records retention policies and protocols that provide additional information specific to the bureau or an individual program. In general, it is illegal to destroy or dispose of any DOHMH record within the retention timeframe established in the DOHMH Records Retention Schedule.

In most cases, once a document is scanned and saved to the appropriate electronic database, the paper document can be disposed of. Paper documents that do not fall under the jurisdiction of the Records Retention Schedule (e.g., duplicate documents, printouts of electronic records, documents scanned to or otherwise recorded in electronic systems, most draft documents) but that contain confidential information must be shred using a DOHMH cross-cutting shredder once no longer needed.

VII. BREACHES AND VIOLATIONS

A breach of confidentiality is an instance in which confidential information is improperly released, misplaced, or stolen, or where there is evidence of willful or intentional misuse. Breaches can be intentional (e.g., viewing a test result for a friend or family member) or inadvertent (e.g., mailing a lab report to the wrong patient or faxing to the wrong number). A violation is defined as a failure to follow policies and procedures which may raise the risk of a breach occurring. A violation may or may not lead to a breach, and a breach can occur in the absence of a violation.

A. Protocol for Addressing a Breach or Violation

The protocol for addressing breaches and violations is presented in the DOHMH Confidentiality Policy and varies depending on the type of breach or violation.

Staff members must report to their immediate supervisor within one hour of detecting a potential or actual violation or breach, whether intentional or inadvertent. If unable to report to the supervisor, staff members should report the potential or actual breach or violation to their DCC or the CPO. Supervisors must ensure the reporting staff member completes an incident report and should consult with the bureau DCC regarding next steps. The bureau DCC must notify the Division DCC of all breaches via email, and collaborate with the CPO on all investigations.

Depending on the type of identifying information that may have been released and the risk to identity security, the agency may be legally obligated to inform the individual(s) of concern and provide them with a year of credit reporting to ensure against identify theft; the decision of whether such steps are necessary will be made by the CPO. In some cases, as with a breach of HIV-related information, New York State and CDC are required to be notified of the breach.

B. Consequences of Violations

Violations of confidentiality rules are considered very serious infractions of New York State law, the NYC Health Code, DOHMH and Division policies and procedures, the City of New York Standards of Conduct, and, sometimes, Federal law. Violations will be evaluated on a case-by-case basis and may lead to a warning, civil or criminal charges, disciplinary action, suspension, remedial training, revocation of access, a change in work assignment, increased shadowing by a supervisor or colleague, termination of employment, referral to legal authorities, or any combination of the above.

EXHIBIT A

LAWS, RULES, AND REGULATIONS GOVERNING CONFIDENTIALITY

The following laws, rules, and regulations may be referred to as necessary for additional information. This is not intended to be an exhaustive list of relevant law. Questions regarding this policy or the interpretation of relevant law should be directed to the bureau Designated Confidentiality Coordinator (DCC), who will consult with the Office of the General Counsel as necessary. Links are current as of the time of publication of this policy and do not link to the official version of the law.

New York City

NYC Health Code, Article 11 (Reportable Disease and Conditions). Lists basic provisions related to reporting, control, and confidentiality. Available at:

<https://www1.nyc.gov/assets/doh/downloads/pdf/about/healthcode/health-code-article11.pdf>

NYC Mayor's Executive Order Nos. 34 and 41. Prohibits staff from inquiring regarding or disclosing immigration status except in limited circumstances. Available at:

<http://www1.nyc.gov/assets/immigrants/downloads/pdf/eo-34.pdf>;
http://www.nyc.gov/html/records/pdf/executive_orders/2003EO041.pdf

New York State

New York State HIV Confidentiality Law, Article 27F. Provides confidentiality requirements for HIV-related information. Available at: <http://law.justia.com/codes/new-york/2010/pbh/article-27-f>

New York State Public Health Law, Article 21, Title 3. Provides confidentiality requirements for HIV-related information. Available at: <http://codes.findlaw.com/ny/public-health-law/#!tid=N4B42A82E2DFF49DCB0378C84FD12724C>

New York State Sanitary Code, Part 63. Provides confidentiality requirements for HIV-related information. Available at: <http://www.health.ny.gov/professionals/ems/pdf/srgpart63.pdf>

New York State Public Health Law 2221. Outlines confidentiality of tuberculosis records and information acquired or maintained by state and local health departments. Available at: <http://codes.findlaw.com/ny/public-health-law/pbh-sect-2221.html>

Federal

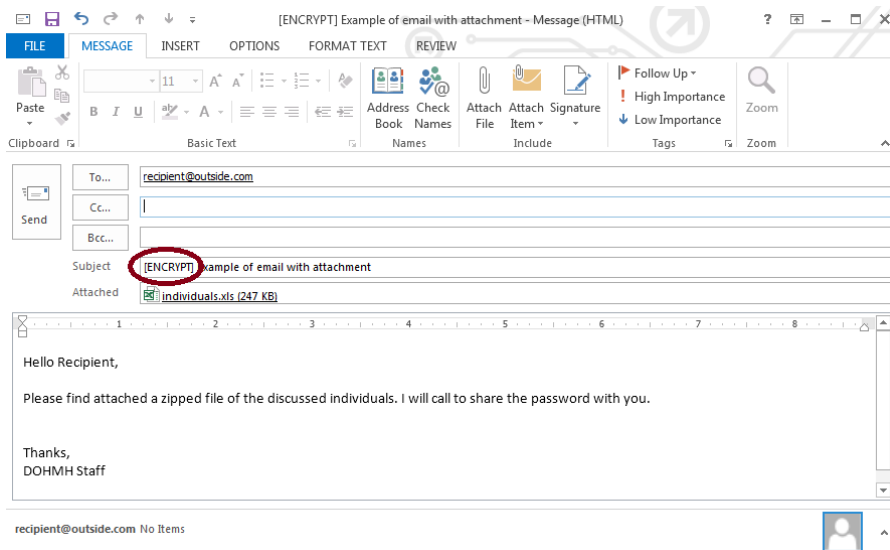
The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Federal law protecting individually-identifiable health information that is held or transmitted by a covered entity (healthcare providers, healthcare clearinghouses, and health plans). Available at: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html>

Exhibit B

Instructions for Password-Protecting Files and Encrypting Emails

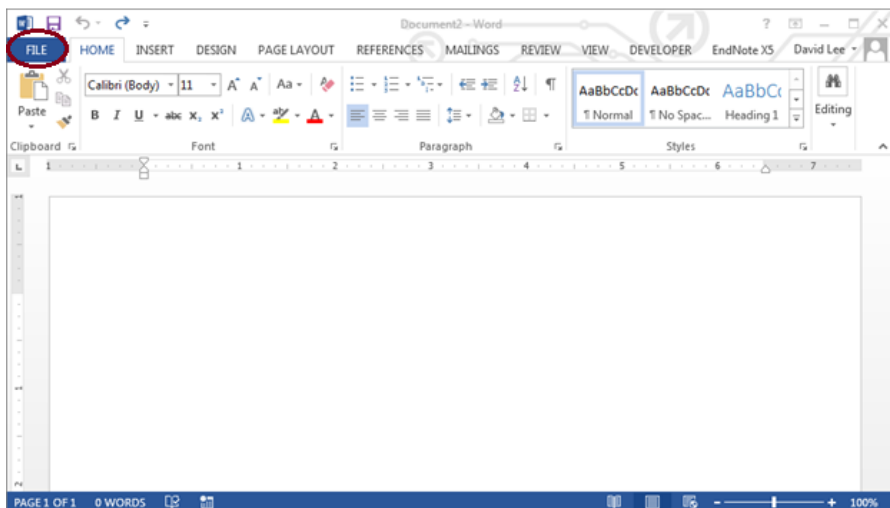
Encrypt an email

1. Ensure that **[ENCRYPT]** is typed in the Subject line of the email.
2. Attach the password-protected file to the email.
3. Call recipient to communicate password over the phone.

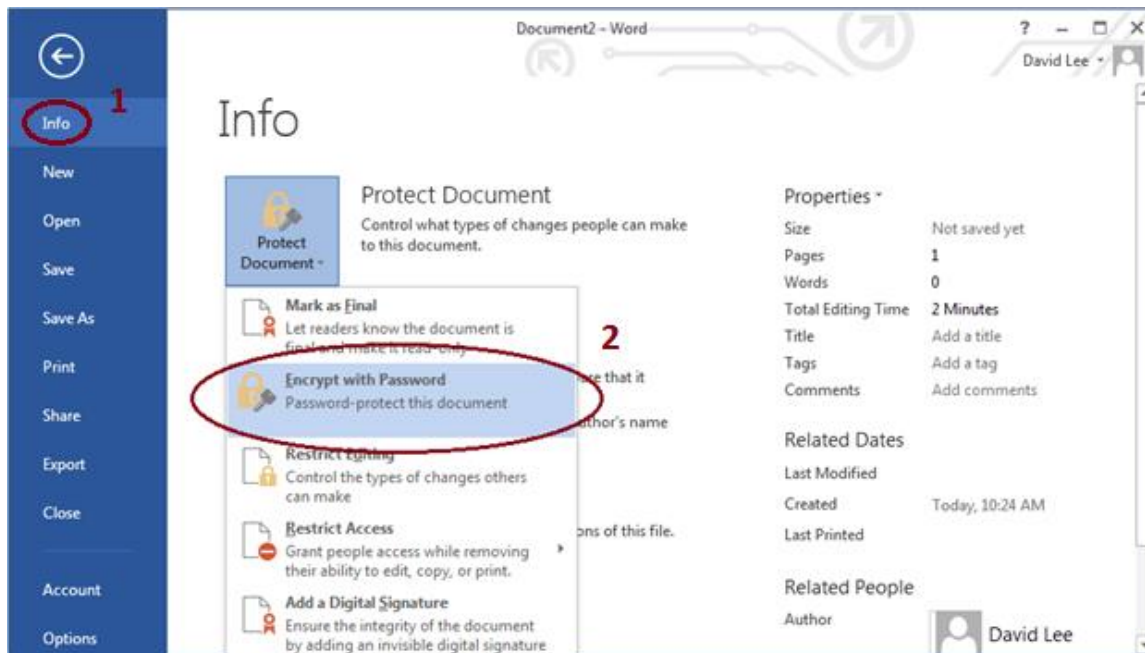


Add a password to protect a Microsoft Office file

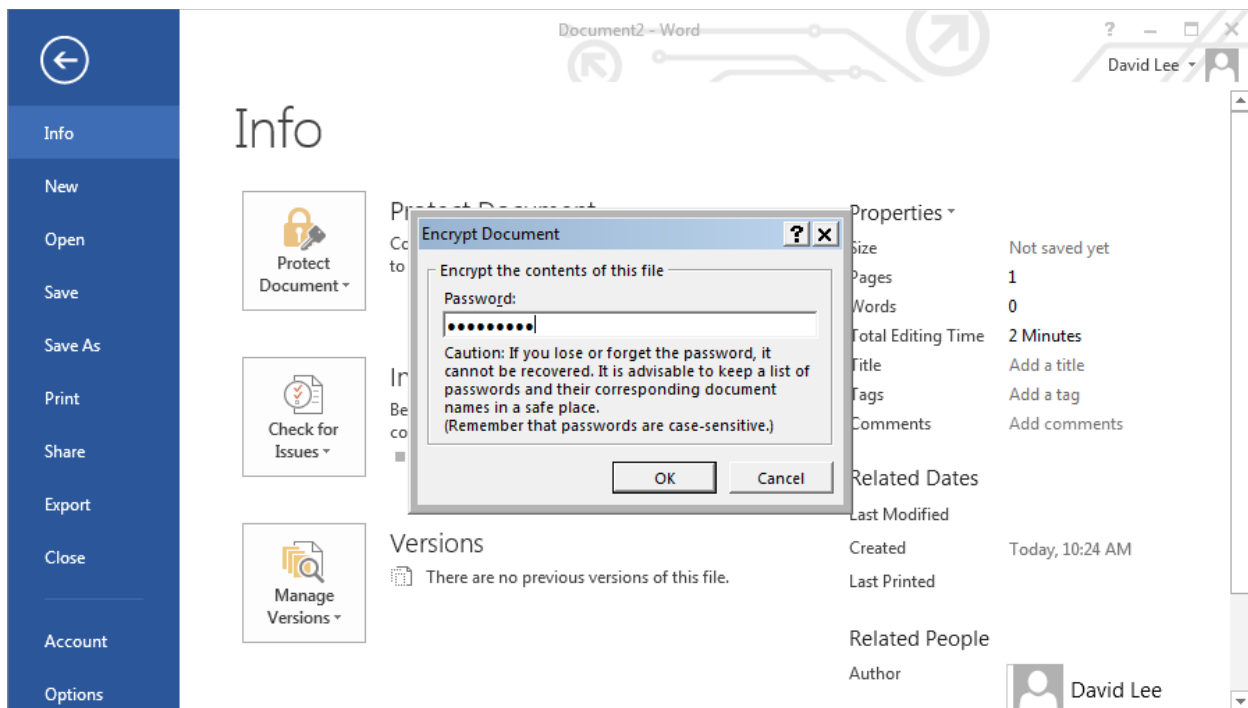
1. Open the file in Microsoft Word or Excel file.
2. Click on **FILE** located in the top-left of the screen in the menu bar.



3. Make sure the **(1) Info** tab is active.
4. Click on the **(2) Protect Document** button. This will reveal a drop-down menu of options.
5. Click on **Encrypt with Password**.



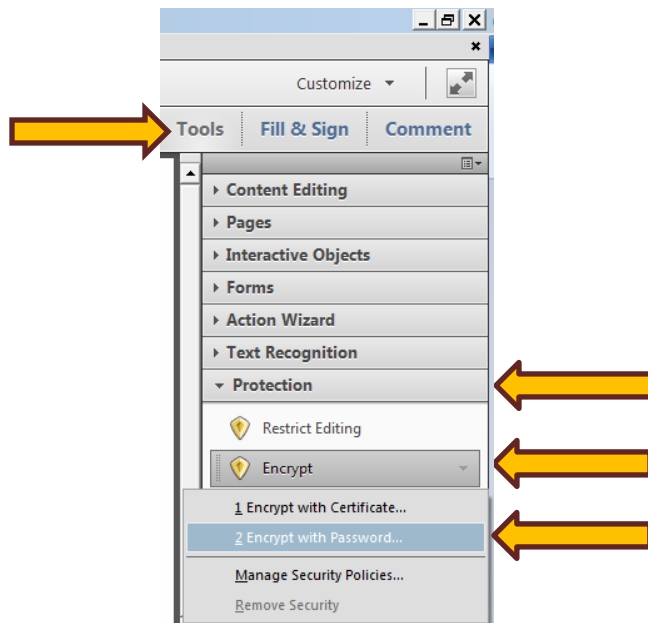
6. Enter a password and click OK.



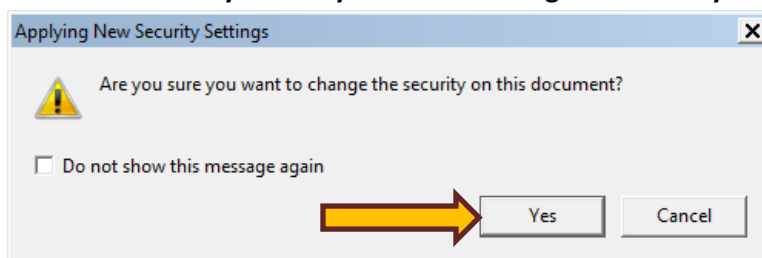
Add a password to protect a PDF file

Applying password to access PDF file

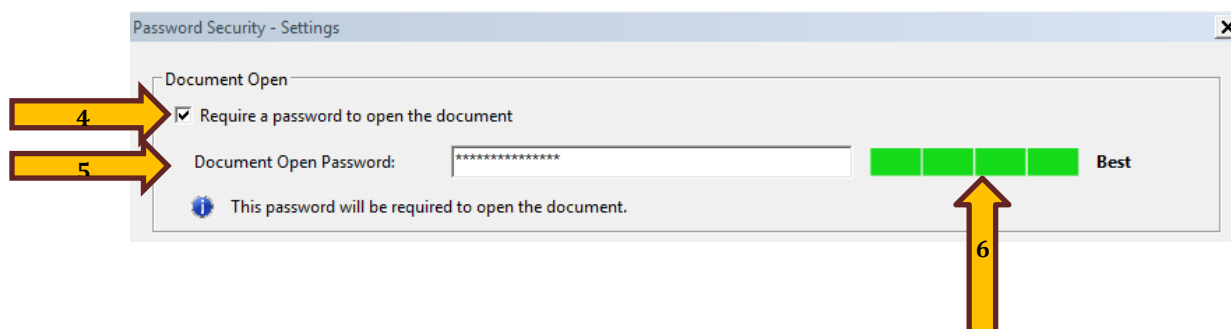
1. Open the PDF File in **Adobe Acrobat Pro**.
2. Select **Tools > Protection > Encrypt** menus on the right side and choose “**Encrypt with Password...**”



3. When asked “**Are you sure you want to change the security on this document?**” click “**Yes.**”



4. In the **Password Security – Settings** window, under “**Document Open**” section, click to put a check mark next to “**Require a password to open the document.**”
5. Enter a password of your choice next to “**Document Open Password.**”



6. The meter to the right of the password will rate how strong the password is.

- a. “**Not Rated**” – No password has been entered



- b. “**Weak**”



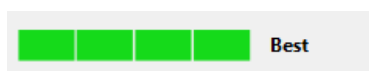
- c. “**Medium**”



- d. “**Strong**”



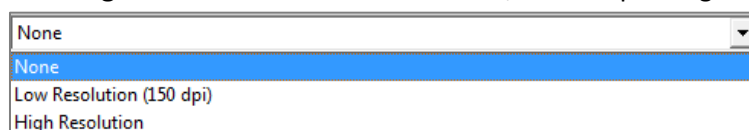
- e. “**Best**”



Applying password to restrict changing permissions

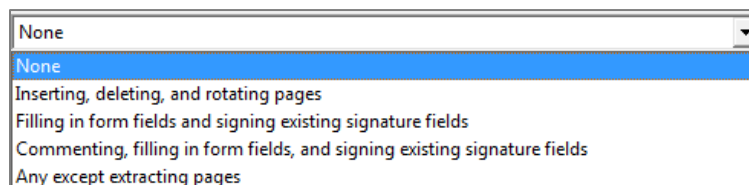
7. In the “**Permission**” section, click to on the check mark next to “**Restrict editing and printing of the document**” this will require a different password in order for person to change the permission settings.
8. Set “**Printing Allowed**” and “**Changes Allowed**” for the restriction level.

- a. **“Printing Allowed”** – if **“None”** is selected, then no printing is allowed.



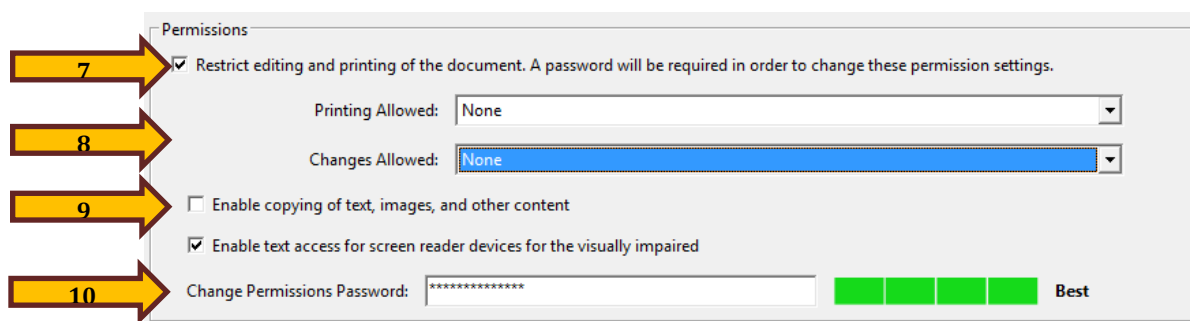
A screenshot of a dropdown menu for 'Printing Allowed'. The menu is open, showing four options: 'None' (highlighted in blue), 'Low Resolution (150 dpi)', and 'High Resolution'. The dropdown arrow is visible on the right side of the menu.

- b. **“Changes Allowed”** – if **“None”** is selected, then no changes allowed without the permission password.



A screenshot of a dropdown menu for 'Changes Allowed'. The menu is open, showing five options: 'None' (highlighted in blue), 'Inserting, deleting, and rotating pages', 'Filling in form fields and signing existing signature fields', 'Commenting, filling in form fields, and signing existing signature fields', and 'Any except extracting pages'. The dropdown arrow is visible on the right side of the menu.

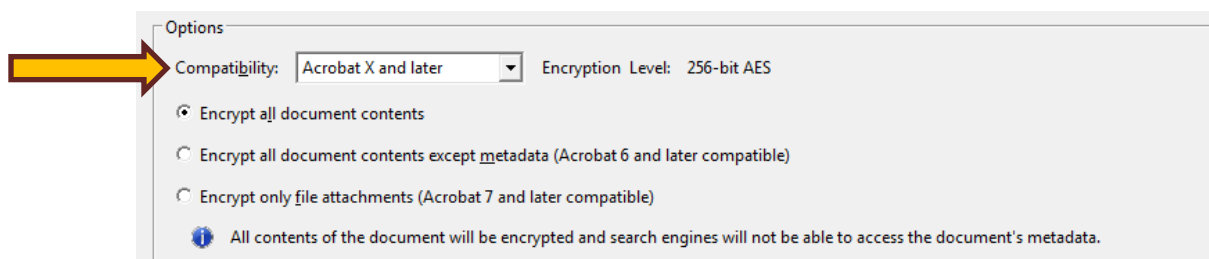
9. Check **“Enable copying of text, images, and other content”** if copying is allowed. If not, leave it unchecked.
10. Enter a different password that can be used to perform all the actions that are restricted or make changes to permission settings.



A screenshot of the 'Permissions' dialog box. Four yellow arrows with numbers 7, 8, 9, and 10 point to specific elements: Arrow 7 points to the 'Restrict editing and printing of the document' checkbox; Arrow 8 points to the 'Printing Allowed' dropdown menu; Arrow 9 points to the 'Enable copying of text, images, and other content' checkbox; Arrow 10 points to the 'Change Permissions Password' text field. The 'Change Permissions Password' field contains a masked password '*****' and a 'Best' button.

Setting encryption level

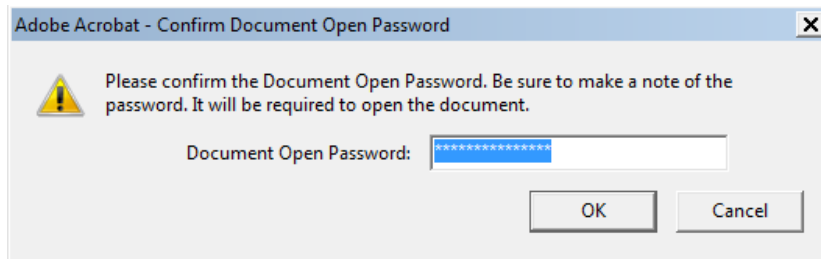
11. In the **“Options”** section, next to **“Compatibility:”** you may select **“Acrobat X and later”** to encrypt the file with the more advanced encryption level, but the file recipient will be required to use **Acrobat or Reader version 8 or later** to open the PDF.



A screenshot of the 'Options' dialog box. A yellow arrow points to the 'Compatibility' dropdown menu, which is set to 'Acrobat X and later'. The 'Encryption Level' is set to '256-bit AES'. Below the dropdown, there are three radio button options: 'Encrypt all document contents' (selected), 'Encrypt all document contents except metadata (Acrobat 6 and later compatible)', and 'Encrypt only file attachments (Acrobat 7 and later compatible)'. At the bottom, there is an information icon and a note: 'All contents of the document will be encrypted and search engines will not be able to access the document's metadata.'

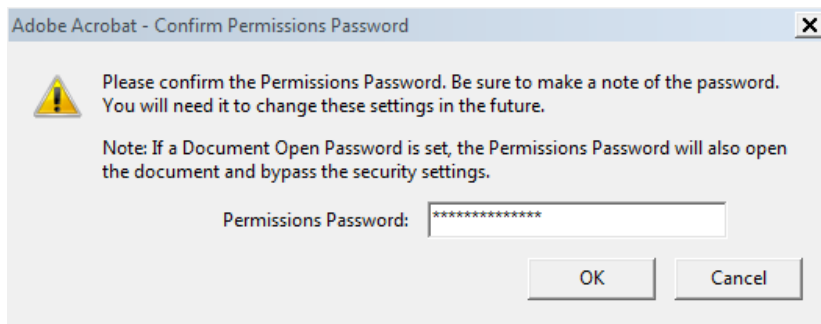
12. Click on **OK**.

13. Re-enter the password created under the “**Document Open**” section to confirm the password.



14. Click **OK**.

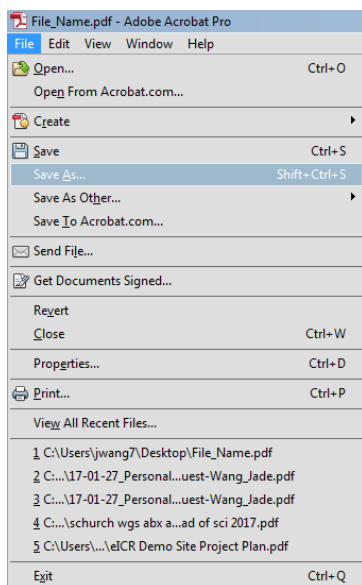
15. If a password is created under the “**Permissions**” section, re-enter the password created under “**Permissions**” section to confirm the password.



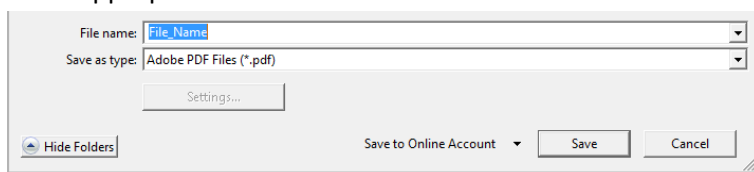
16. Click **OK**.

Save the PDF file to save changes

17. Select **File > Save As**.

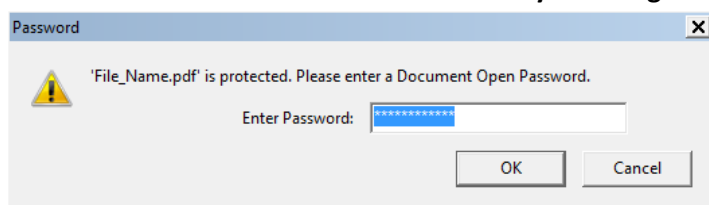


18. Enter appropriate file name next to **“File Name”** and click **“Save”**.



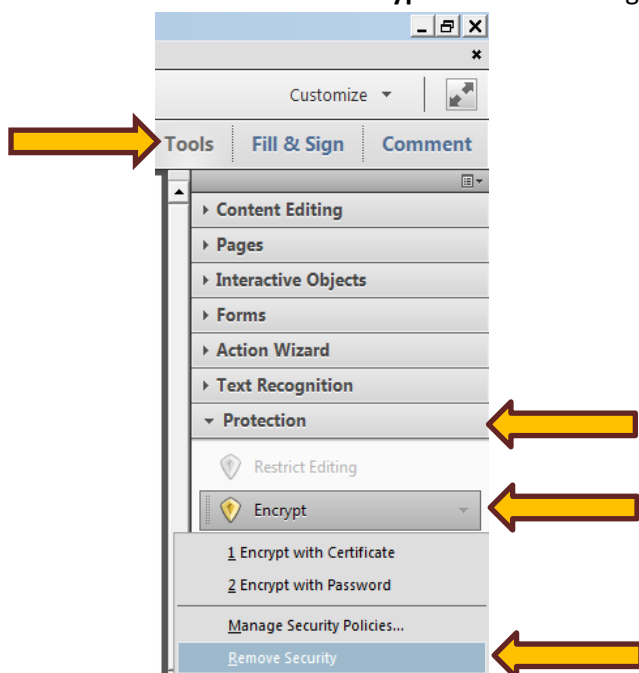
Open files with “Document Open Password” protection

1. Upon opening a password-protected file, enter the password created in the **“Document Open Password”** section of the **“Password Security – Settings”**.



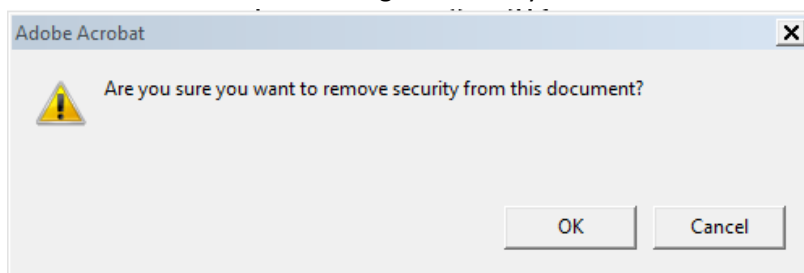
Remove password security from a document

1. Select **Tools > Protection > Encrypt** menus on the right side and choose **“Remove Security”**.



2. System will require the **“Permission Password”** if one was created in the **“Permission”** section of **“Password Security – Settings”**.

3. Click on **OK** to confirm removing the security from the document.



4. Save the PDF file to confirm changes.

Questionnaire Required for all Contract-Related Requests Involving Data Sharing between Internal City Agencies

This questionnaire provides the Law Department with necessary information to perform a privacy review of City initiatives. The initiatives may involve (1) data collection from one or more City departments, units, divisions or contracted providers ("agencies")¹. These initiatives may result in a review/creation/modification of a memorandum of understanding and/or a review of a data licensing agreement.

Date of Request: _____ / ____ /20____
Requestors Name: _____
Name of Project manager: _____
City Agency: _____
Telephone No.: _____
Email: _____

Priority Level (Check one): ☐ Low: _____ ☐ Moderate: _____ ☐ High _____
(Estimated deadline) (Estimated deadline) (Estimated deadline)

In the section below, identify all additional agencies that may be involved with the request.

Name of Contact Person: _____	Name of Contact Person: _____
City Agency: _____	City Agency: _____
Telephone No.: _____	Telephone No.: _____
Email: _____	Email: _____
Providing data: Yes/No	Providing data: Yes/No
Receiving data: Yes/No	Receiving data: Yes/No

Name of Contact Person: _____	Name of Contact Person: _____
City Agency: _____	City Agency: _____
Telephone No.: _____	Telephone No.: _____
Email: _____	Email: _____
Providing data: Yes/No	Providing data: Yes/No
Receiving data: Yes/No	Receiving data: Yes/No

1. Type of Initiative.

a. Identify the purpose of the request by checking the appropriate box below:

- ☐ Providing services
- ☐ Coordinating services among agencies
- ☐ Program Evaluation
- ☐ Research and Scholarship
- ☐ Policy Development
- ☐ Administration of the Health Choices program (required for Medicaid data)
- ☐ Other: _____

¹ Department of Behavioral Health and Intellectual Disability Services, Philadelphia Department of Public Health, Office of Homeless Services, Emergency Medical Services, Department of Human Services, Office of Human Resources, Data Management Office, Philadelphia Police Department and Philadelphia Prisons.

This image shows a single sheet of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper has a slightly textured appearance and is set against a dark background.

a. Please check all that apply:

The types of data that will be shared are:

- b. Complete the below chart listing all data elements that will be shared, identifying each City agency whose data will be used or accessed and the system from which each data element will be extracted:**

DEPARTMENT	DIVISION/SERVICE PROVIDER (if applicable)	DATA SYSTEM ²	DATA ELEMENTS ³

3. Check only one:

- ☐ The data collected will only be shared in one direction (from the data source(s) to the recipient(s)).
- ☐ The data collected will be shared in two directions (agencies will contribute data and receive data for the initiative).

4. Access to the data.

a. Is there a contractual relationship between the agencies providing data and receiving data for this initiative? Note: For purposes of this question, a contractual relationship may include an executed contract between the City agency and an external agency or an MOU between two City agencies.

b. List all internal persons or City agencies that will have access to the data:

Name(s) of internal parties: **Is there an MOU covering this initiative? (circle Yes or No):**

_____	Yes/No
_____	Yes/No
_____	Yes/No
_____	Yes/No
_____	Yes/No
_____	Yes/No

c. External access to the data. Check all that apply.

- ☐ External persons or entities will have access to the data.

The external parties are: **Is the external party under City contract? (circle your Yes or No):**

_____	Yes/No
_____	Yes/No
_____	Yes/No

d. Embedded contract staff.

- ☐ Embedded contract staff will have access to the data.

The contracted entities are:

5. Where will the data be stored?

² An example of a data system is eCW.

³ Examples of data elements are age in years or gender.

6. How will the data be transferred between parties?

7. How long will the data be retained?

8. How will the data be handled after the initiative is completed?

9. Consent. Check all that apply.

- ☐ This program or initiative will include the collection of individual consent forms that authorize the identified agencies to share the data.
- ☐ I have attached a copy of the draft consent form.
- ☐ I require assistance drafting the consent form.
- ☐ I plan to share the data without obtaining individual consents. If checked, please explain why the data will be shared without consents.

10. Court Order. Check one.

- ☐ There will be a court order to disclose or share the data.
- ☐ There will not be a court order requiring data to be shared.

Please send completed form and all attachments to hipaaprivacy@phila.gov.

GOBIERNO DE PUERTO RICO
DEPARTAMENTO DE SALUD
SAN JUAN, PUERTO RICO

ACUERDO COLABORATIVO ENTRE EL DEPARTAMENTO DE SALUD Y _____
PARA EL INTERCAMBIO DE DATOS

COMPARECEN

DE LA PRIMERA PARTE: El DEPARTAMENTO DE SALUD, representado por el Secretario de Salud, **RAFAEL RODRÍGUEZ MERCADO, MD, FAANS, FACS**, mayor de edad, casado, médico de profesión y vecino de **GUAYNABO, Puerto Rico**, o representado por la Sub Secretaria de Salud, **CONCEPCIÓN QUIÑONES DE LONGO, MD**, mayor de edad, casada y vecina de Guaynabo, Puerto Rico, quien comparece en representación del Secretario de Salud y está autorizada a firmar contratos en virtud de la delegación hecha por el Secretario en comunicaciones fechadas 3 y 18 de enero de 2017, de conformidad con la Ley Núm. 81 de 14 de marzo de 1912, según enmendada, en adelante denominada la **PRIMERA PARTE**.

DE LA SEGUNDA PARTE: _____ una corporación debidamente autorizada a hacer negocios al amparo de las Leyes del Estado Libre Asociado de Puerto Rico, representada por _____, en su capacidad como _____, mayor de edad, casado/soltero y vecino de _____ Puerto Rico, en adelante denominada la **SEGUNDA PARTE**.

EXPONEN

PRIMERO: La misión del Programa de Vacunación de la **PRIMERA PARTE** es prevenir el desarrollo de enfermedades a través de la vacunación temprana y cimentada en el fortalecimiento del Itinerario de Vacunación para Niños, Adolescentes y Adultos de Puerto Rico, así como en la implementación de estrategias eficaces de intervención que permitan facilitar los servicios de vacunación a la población en general.

SEGUNDO: La visión es tener una población protegida contra las enfermedades prevenibles por vacunas, reduciendo los surgimientos de brotes, hospitalizaciones y muertes. Para lograr lo anterior se necesita la implementación de diversas estrategias que así lo faciliten. Una de estas es mantener actualizado el *Registro de Vacunación de Puerto Rico (PRIR)*, por sus siglas en inglés) con la información de toda la población Puerto Rico.

TERCERO: El *Registro de Vacunación de Puerto Rico (PRIR)*, fue diseñado para ser utilizado a través del Internet, con el fin de agilizar los trámites de vacunación de una manera segura y sobre todo confidencial. La **PRIMERA PARTE** se asegura que el *PRIR* cumpla con todos los requisitos federales y estatales requeridos. El *PRIR* permite identificar las necesidades de vacunación por proveedor y área geográfica, facilitando así mantener niveles de cobertura óptimos en todo Puerto Rico.

CUARTO: Información de la **SEGUNDA PARTE**.

QUINTO: **AMBAS PARTES** convienen realizar un Acuerdo con el fin de consolidar la información de vacunación de la **PRIMERA PARTE** y de la **SEGUNDA PARTE**. Este Acuerdo consiste en el intercambio de datos de vacunación entre las **PARTES**. Mediante el intercambio de datos se pretende lograr un aumento en los expedientes con información de vacunación completada no solo en la población registrada en el *PRIR*, sino en el sistema de la **SEGUNDA PARTE**. Además, permite identificar y vacunar a personas que no tienen sus vacunas al día, lo cual será un beneficio para toda la población.

SEXTO: Conforme a lo anteriormente expuesto, **AMBAS PARTES** acuerdan suscribir el presente Acuerdo con forme a las siguientes:

CLÁUSULAS Y CONDICIONES

PRIMERA: El proceso de intercambio de datos constará de un periodo de pruebas para asegurar la calidad de los datos exportados al *Registro de Vacunación de Puerto Rico (PRIR)*. Se procederá como sigue:

- La **PRIMERA PARTE** suministrará la Guía Local de Implementación de Mensajes de Inmunización HL7 versión 2.5.1 a la **SEGUNDA PARTE**.
- La **SEGUNDA PARTE** deberá crear los archivos de pruebas utilizando los requerimientos especificados en la Guía Local de Implementación de Mensajes de Inmunización. Estos deberán de incluir un mínimo de cinco (5) récords y serán enviados a la persona encargada de la **PRIMERA PARTE**.
- La **PRIMERA PARTE** revisará y exportará los archivos al sistema *PRIR*. De ocurrir algún error en el formato, la persona encargada de la **PRIMERA PARTE** se comunicará vía correo electrónico o

teléfono con la persona encargada de la **SEGUNDA PARTE** para notificar sobre el particular para la corrección del archivo.

SEGUNDA: El proceso antes descrito se repetirá hasta tanto el archivo cumpla con todos los parámetros requeridos de calidad de los datos del *Registro de Vacunación de Puerto Rico (PRIR)*. Una vez completada esta fase, se procederá como sigue:

- El personal responsable de la **PRIMERA PARTE** creará una cuenta de usuario a la persona asignada de la **SEGUNDA PARTE** para que pueda acceder al *PRIR*. La **SEGUNDA PARTE** firmará los Acuerdos de Confidencialidad y Seguridad necesarios para acceder al *PRIR*.
- El personal de la **SEGUNDA PARTE** creará archivos con los datos de vacunación de los asegurados siguiendo los parámetros utilizados en los archivos de prueba y los exportará al *PRIR*.
- La persona encargada de la **PRIMERA PARTE** monitoreará que los archivos exportados por la **SEGUNDA PARTE** cumplan con los requisitos de calidad de los datos del *Registro de Vacunación de Puerto Rico (PRIR)*. De ocurrir algún error y/o situación con algún archivo, el personal encargado se comunicará vía correo electrónico o teléfono con el personal de la **SEGUNDA PARTE** para notificar sobre la situación para su debida corrección.
- A solicitud de la **SEGUNDA PARTE**, el personal de la **PRIMERA PARTE** preparará un archivo en formato “*Flat File*” el cual incluirá todos los datos de vacunación correspondiente a los asegurados de la **SEGUNDA PARTE**. El archivo será enviado a la encargada de la **SEGUNDA PARTE**.

TERCERA: Las personas encargadas y responsables del intercambio de los datos serán:

- | | |
|--|--|
| <ul style="list-style-type: none">• Norma Castro Monge
Analista de Programa
Programa de Vacunación
Departamento de Salud | Teléfono: 787.765.2929 Ext.3329
Correo electrónico: norma.castro@salud.pr.gov |
| <ul style="list-style-type: none">• Verónica Rodríguez
Supervisora de Sistemas
Programa de Vacunación
Departamento de Salud | Teléfono: 787.765.2929 Ext.3326
Correo electrónico: vrodriguez@salud.pr.gov |
| <ul style="list-style-type: none">• Persona contacto Aseguradora | Teléfono:
Correo electrónico: |

CUARTA: AMBAS PARTES reconocen que está prohibido el uso de los datos provistos para cualquier otro propósito no explícitamente identificado y aprobado en este Acuerdo de intercambio de datos.

QUINTA: LEY FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT DE 1996:

- A. La ley federal Health Insurance Portability and Accountability Act del 1996 (mejor conocida por sus siglas en inglés HIPAA) y su Regla de Privacidad y Seguridad requieren que toda entidad cubierta por dicha legislación adiestre a su fuerza laboral y establezca Políticas y Procedimientos en cuanto a las disposiciones sobre la privacidad, confidencialidad y seguridad de la información de salud de los pacientes, sea dicha información creada, almacenada, manejada, accesada o transmitida en papel o por medios electrónicos.
- B. HIPAA define su fuerza laboral como aquellos empleados regulares, por contrato, transitorios, voluntarios, estudiantes, practicantes y cualquier persona que lleve a cabo una labor en el área asignada por la **PRIMERA PARTE**, sea o no remunerada.
- C. La **SEGUNDA PARTE** es una entidad cubierta bajo la reglamentación de HIPAA 164.103 (1) (i)(11)(2) y el Omnibus Rule” (e) 164.400 y como tal, está sujeta al cumplimiento de sus propias políticas y procedimientos establecidos por la **PRIMERA PARTE** para el cumplimiento con la Ley HIPAA y su reglamentación relacionada. A tales efectos:
 - i. La **SEGUNDA PARTE** adiestrará a sus empleados sobre dicha ley, su Regla de Privacidad, Códigos, Transacciones e Identificadores y su Regla sobre la Seguridad de la Información de Salud que es accesada, creada, mantenida, o transmitida por medios electrónicos (ePHI).
 - ii. Conocer y obligarse a cumplir con los términos establecidos en la Política y Procedimientos Sobre Prácticas de Privacidad y Seguridad de la **PRIMERA PARTE**.

- iii. Informar de inmediato a la **PRIMERA PARTE**, por escrito, de cualquier uso y/o divulgación de la información de salud protegida de los pacientes que no cumpla con los términos de este contrato. 45 C.F.R. §164.504(e)(2)(ii)(C), según establecido en las disposiciones del “Omnibus Rule”.
 - iv. La **SEGUNDA PARTE** deberá asegurarse de que cualquier agente o subcontratista suyo cumpla con las mismas condiciones que tiene como responsabilidad de cumplir bajo las enmiendas del “Omnibus Rule” de HIPAA.
 - v. En caso de que la **SEGUNDA PARTE** tuviere que divulgar a terceros información de salud protegida de los pacientes, para efectos de cumplir con los términos y condiciones de este acuerdo y sus deberes y responsabilidades bajo el mismo, antes de divulgar la información obtendrá una seguridad razonable y adecuada de dicho TERCERO, de que la información se mantendrá confidencial y segura, que sólo será divulgada según requerido por ley y únicamente para los propósitos para los que le fue divulgada y de que notificará de inmediato a la **PRIMERA PARTE** cualquier violación a la confidencialidad de la información de que tenga conocimiento. 45 C.F.R. §§164.504(e)(2)(i), §§164.504(e)(2)(i)(B), §§164.504(e)(2)(ii)(A) y §§164.504(e)(4)(ii).
 - vi. Cumplir con todas sus políticas y las de la **PRIMERA PARTE** para la protección de la privacidad, confidencialidad y seguridad de la información de salud de los pacientes, se encuentre esta información en papel o por medios electrónicos. Cumplir con la reglamentación federal para el manejo y custodia de la información de salud protegida, (electronic Protected Health Information, en adelante e-PHI por sus siglas en inglés), en relación al aspecto administrativo, físico y técnico según estatuido en el 45 CFR secs. 164.308, 164.310, 164.312, 164.316).
- D. En cuanto al manejo de la información de salud protegida, PHI que comparten **LAS PARTES**, se requerirá de la **SEGUNDA PARTE** los siguientes estándares para el manejo de PHI:
- 1. Mantener sistemas que protejan la información de salud protegida, ya sea por medios físicos y/o electrónicos Protected Health Information (PHI) y Electronic Protected Health Information (ePHI), contra accesos no autorizados y mantener el cumplimiento con las reglas de seguridad electrónicas de HIPAA, incluyendo pero no limitado a la elaboración de un análisis de riesgo electrónico.
 - 2. La **SEGUNDA PARTE** podrá permitir al individuo, dueño del PHI, accesos a su información de salud. La **SEGUNDA PARTE** cumplirá con HIPAA y la Política de la **PRIMERA PARTE** de divulgar solamente el mínimo necesario a la solicitud de información.
 - 3. Llevar un registro de la información de salud protegida que divulga, del cual deberá tener libre acceso la **PRIMERA PARTE** y mostrado según requerido por esta ultima 45 CFR &164.528.
 - 4. Informar de inmediato a la **PRIMERA PARTE**, cualquier uso o divulgación no autorizada tan pronto tenga conocimiento de este hecho.
 - 5. Incorporar cualquier enmienda a la información de un individuo que le sea transmitida por la **PRIMERA PARTE**.
 - 6. Poner a la disposición del Departamento de Salud y Servicios Humanos Federal (Department of Health and Human Services, DHHS por sus siglas en inglés), sus prácticas internas, libros y expedientes relacionados con el uso y divulgación de información protegida recibida de la **PRIMERA PARTE**.
 - 7. Las partes se devolverán entre sí aquella información de salud protegida en su formato físico y/o electrónico, que haya sido suministrada para el cumplimiento de los términos contenidos en este acuerdo. No obstante lo anterior, las Partes podrán retener aquella información que deban retener (i) para cumplir con sus respectivas obligaciones ante la ley, reglamento o políticas aplicables a la retención de documentos, e (ii) información que ha sido almacenada en los sistemas de resguardo electrónico de la parte que retiene la información y no es razonablemente posible su destrucción. La parte que retiene la información se mantendrá completamente responsable del cumplimiento de las obligaciones de confidencialidad que surgen de este acuerdo con relación a toda la información que retenga en virtud de esta cláusula.
 - 8. Las Partes serán responsables de la seguridad e integridad de la información de salud protegida compartida, en particular, incluyendo aquella que sea compartida por herramientas tecnológicas

("devices") y medios electrónicos móviles. En particular, las Partes, cumplirán con los siguientes requisitos:

- a. La información de salud será compartida entre las Partes por las plataformas electrónicas que proveerá la **PRIMERA PARTE** para tales fines.
 - b. No obstante lo anterior, si las Partes comparten información de salud protegida por otros mecanismos electrónicos, incluyendo pero sin limitarse a correo electrónico y dispositivo móviles, las Partes representan mediante este acuerdo que dichos mecanismos electrónicos poseen salvaguardas suficientes para proteger la confidencialidad e integridad de la información compartida, incluyendo implementación de contraseñas y mecanismos de cifrado electrónico y/o aquella forma de protección que sea factible o accesible a las partes.
 - c. Ambas partes restringirán el intercambio de información de salud a aquellas plataformas electrónicas diseñadas para compartir la información de salud objeto de este acuerdo evitando así utilizar herramientas tecnológicas móviles ("devices") privados tales como: Teléfonos celulares; Computadoras portátiles, memorias portátiles, discos portátiles, entre otros.
- E. **AMBAS PARTES** serán responsables de cumplir con lo dispuesto en la Subparte C del 45 CFR § 164 relativo al cumplimiento con la protección de la información de salud que se maneja por métodos electrónicos. Deberá informar de inmediato a la otra Parte tan pronto tenga conocimiento sobre cualquier uso o divulgación de información de salud protegida no autorizada, así como de informar cualquier incidente de seguridad electrónica en la cual se pueda ver expuesta la información de salud de los participantes y pacientes según requerido por 45 CFR § 164.410. La Parte que haya incumplido con lo aquí dispuesto será responsable de costear los gastos que puedan generarse en caso de una violación al manejo de información de salud protegida en su forma física y/o electrónica.
- F. Cada Parte será responsable con su propio pecunio, de notificar a cada uno de los pacientes y participantes de que ha ocurrido un incidente de seguridad electrónica que afecta o compromete su información de salud, y procederá a reportar el incidente de seguridad a la Oficina de Derechos Civiles del Departamento de Salud Federal, (OCR), Health and Human Services) en cumplimiento con la Health Information Technology for Economic and Clinical Health ACT, (HITECH) y la Genetic Information Nondiscrimination ACT, (GINA), según le sea requerido por ley, y dará cuentas de dichas gestiones a la otra Parte mediante informe que incluya todas las gestiones realizadas para la solución del incidente. La **SEGUNDA PARTE** deberá notificar a la Oficina de Administración y Monitoreo de la HIPAA del Departamento de Salud de Puerto Rico, según le sea aplicable.
- G. De una Parte no cumplir con los estándares establecidos tanto en la ley federal HIPAA, como en su reglamentación relacionada, las leyes estatales que protegen la privacidad, confidencialidad y seguridad de la información de salud de los pacientes y, en el caso de la **SEGUNDA PARTE**, con las Políticas y Prácticas de Privacidad y Confidencialidad y Seguridad de la **PRIMERA PARTE**, la otra Parte se expone a ser sancionado por el **DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)** y este Acuerdo puede ser terminado inmediatamente. Ambas Partes se reservan el derecho de resolver este Acuerdo conforme establecido en la **CLAUSULA DE VIGENCIA Y RESOLUCION** de este Acuerdo.
- H. La **SEGUNDA PARTE** reconoce que de existir una violación a las leyes Federales, su reglamentación, así como a la legislación local en cuanto al manejo de información de salud protegida, sea física o material, será responsable de pagar aquella(s) multa(s) que por dicho concepto imponga el Departamento de Salud Federal así como la Oficina de Derechos Civiles ("OCR", por sus siglas en inglés) que sean directamente relacionadas al incumplimiento de la **SEGUNDA PARTE** con el manejo adecuado de la información de salud protegida que contempla este Acuerdo.

SEXTA: VIGENCIA Y RESOLUCIÓN: Este Acuerdo entrará en vigor a partir de la firma de la **PRIMERA PARTE** y estará vigente hasta el _____. El mismo podrá ser renovado mediante enmienda escrita a esos efectos, firmada por **AMBAS PARTES**. Este Acuerdo podrá ser resuelto antes de su vencimiento por cualquiera de las **PARTES** mediante notificación escrita a la **OTRA PARTE** por correo certificado con acuse de recibo, con treinta días (30) de notificación previa a la fecha de terminación deseada. La notificación será enviada a la siguiente dirección:

Si a la **PRIMERA PARTE**: **DEPARTAMENTO DE SALUD**
PO Box 70184
San Juan, PR 00936-8184

Si a la **SEGUNDA PARTE**:

SÉPTIMA: De alguna de **LAS PARTES** incurrir en negligencia, abandono, incumplimiento de las cláusulas y condiciones del presente Acuerdo, la **OTRA PARTE** podrá disolver el presente Acuerdo mediante previa notificación escrita a la **OTRA PARTE**.

OCTAVA: AMBAS PARTES mantendrán vigente bajo este acuerdo las pólizas de seguro que correspondan a sus operaciones y responderá cada cual con sus propias pólizas por aquellas reclamaciones que puedan surgir relacionadas con este acuerdo.

NOVENA: Los servicios aquí acordados se brindarán libres de costo por **AMBAS PARTES**. *Este Acuerdo no conlleva erogación de fondos.*

DÉCIMA: ULTRAVIRES: CONFORME A DERECHO Y LAS NORMAS QUE RIGEN LA CONTRATACIÓN DE SERVICIOS, LOS COMPARECIENTES EN ESTE ACUERDO TOMAN CONOCIMIENTO DE QUE NO SE PRESTARÁ SERVICIO ALGUNO BAJO ESTE ACUERDO HASTA TANTO SEA FIRMADO POR AMBAS PARTES. DE LA MISMA FORMA, NO SE CONTINUARÁ DANDO SERVICIO BAJO ESTE ACUERDO A PARTIR DE LA FECHA DE SU EXPIRACIÓN, EXCEPTO QUE A LA FECHA DE EXPIRACIÓN EXISTA YA UNA ENMIENDA FIRMADA POR AMBAS PARTES. CUALQUIER FUNCIONARIO QUE SOLICITE Y ACEPTÉ SERVICIOS DE LA OTRA PARTE EN VIOLACIÓN A ESTA DISPOSICIÓN, LO ESTÁ HACIENDO SIN AUTORIDAD LEGAL ALGUNA.

ACEPTACIÓN

AMBAS PARTES aceptan este Acuerdo por estar ajustado a lo convenido y se obligan al cumplimiento de todas sus cláusulas y condiciones.

EN TESTIMONIO DE LO CUAL, LAS PARTES suscriben este Acuerdo obligándose así formalmente a cumplir con todas sus cláusulas y condiciones.

En San Juan, Puerto Rico, hoy ____ de _____ de 2017.

SEGUNDA PARTE
SS:

PRIMERA PARTE
SS: 660-43-7470

CERTIFICACIÓN

Yo, _____ Abogado(a) de la Oficina de Asesores Legales del Departamento de Salud certifico que he revisado el contrato en todos sus pormenores y, he encontrado el mismo satisfactorio desde el punto de vista legal. Recomendando su firma.

Firma: _____ Fecha: _____