March 31, 2009

Health Information Security and Privacy Collaboration

User Guide: Public Health Data Sharing Agreement

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by

Interorganizational Agreements Collaborative
Alaska, Guam, Iowa, New Jersey, North Carolina, South Dakota

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

March 31, 2009

Health Information Security and Privacy Collaboration

User Guide: Public Health Data Sharing Agreement

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by

Interorganizational Agreements Collaborative
Alaska, Guam, Iowa, New Jersey, North Carolina, South Dakota

Identifiable information in this report or presentation is protected by federal law, section 924(c) of the Public Health Service Act, 42 USC. § 299c-3(c). Any confidential identifiable information in this report or presentation that is knowingly disclosed is disclosed solely for the purpose for which it was provided.

User Guide

HISPC Interorganizational Agreement (IOA) for Electronic Health Information Exchange

Public Health-to-Public Health Data Sharing Agreement

Developed by the Interorganizational Agreements Collaborative[1] (IOA) of the Health Information Security and Privacy Collaboration (HISPC) Project
March 2009

This User Guide is for parties using data sharing agreements to enter into electronic health information exchange (eHIE) efforts. Two data sharing agreements for eHIE were developed as part of the HISPC Project. This User Guide is a companion resource to the public-to-public data sharing agreement (Public Health Agreement) and explains the background, rationale, and other considerations related to use of the Public Health Agreement.

Background 2
Mission 2
Development Steps 3
Policy Decisions and Guiding Principles 4
Guidelines for Completing the Public Health Agreement 4
Additional Considerations for the Public Health Agreement 5
Endorsements and/or Review of the Public Health Agreement 5
Frequently Asked Questions (FAQs) 8

[1] The IOA Collaborative and the HISPC Project are explained further in the document.

Background

The IOA data sharing agreements (DSAs) are the result of several years of highly cooperative work among states, territories, and the federal government to resolve unnecessary barriers to interstate, interoperable, private, and secure eHIE. When the Health Information Security and Privacy Collaboration (HISPC) was first established in 2006, 34 states,[2] under the leadership of the prime contractor, RTI International, joined together to conduct a year-long project in which each participant would identify such barriers and propose implementation plans to address these impediments consistent with HIPAA,[3] state privacy and security laws and regulations, and organizational policies.

In the next phase, the HISPC member states formed into groups to take steps to implement a specific project to resolve one of the barriers that had been identified in the earlier HISPC work. Seven Collaboratives were formed under the supervision of the Office of the National Coordinator for Health Information Technology (ONC), one of which is the Interorganizational Agreements Collaborative (IOA). Alaska, Guam, Iowa, North Carolina, New Jersey, and South Dakota[4] are the members of IOA. The Collaborative proposed to address the lack of available DSAs containing consistent privacy and security provisions to support cross-state electronic health information exchange (eHIE).

The third phase of the HISPC project resulted in two DSAs. This User Guide addresses the Public Health Agreement. A companion User Guide similarly addresses the Private Entity-to-Private Entity Data Sharing Agreement. Throughout all phases of the IOA work, the guiding principle has been mutually acceptable resolution of barriers consistent with applicable privacy and security laws and regulations. The overall purpose was to create agreements that could be used throughout the country for standard arrangements that have received significant review and that are consistent among participants.

Mission

The IOA-drafted DSAs can be used in the following situations:

1. Public health agency-to-public health agency exchange of protected health information (PHI) that is held in public health registries pursuant to various federal and state laws. *Information specific to the Public Health Agreement begins with the "Guidelines for Completing the Public Health Agreement" section below.*

2. Private entity-to-private entity exchange of PHI among private entities such as between hospitals, medical centers, regional health information organizations, laboratories, payors, PHRs, and other private organizations. *Information specific to private entity ePHI*

[2] States shall mean states and territories.

[3] HIPAA is the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations on privacy and security, found at 45 C.F.R. Parts 160 and 164.

[4] Two additional states participated in the process but ultimately were not able to continue to participate.

exchanges is found in the Private Entity-to-Private Entity Data Sharing Agreement User Guide, which is a companion to the Private-to-Private Data Sharing Agreement.

Development Steps

The IOA developed a plan to ensure that the final work product would be suitable for use nationwide. Thus, the IOA sought to create a national standard for use in specific types of circumstances, such as sharing public health registry information and provider-to-provider eHIE.

The plan of action included the following steps:

- Approximately 50 documents (memorandums of understanding, DSAs, etc.) were gathered and cataloged by the IOA as source material.
- Each document was carefully reviewed. Each provision in each document was classified according to its provenance and subject matter. Similar provisions from different agreements were then extracted, combined, and placed next to each other in a master document.
- This process resulted in a matrix of more than 350 pages in which similar provisions from the source documents were grouped together for side-by-side comparison. The provision categories included privacy, security, immunity, conflict of law, and numerous other topics.
- This development and review process included coordination and cooperation with the Nationwide Health Information Network (NHIN) Data Use and Reciprocal Support Agreement (DURSA) Work Group.
- The IOA then selected the most effective language and provisions with consideration of any conflicts in state law. This work included review by state-specific legal Work Groups as well as the IOA Collaborative as a whole, which removed any provisions felt to be illegal or ill-advised under state law.
- At the end of this process, the IOA met to draft final templates for public-to-public and private-to-private electronic data sharing.
- The template documents were delivered to participating state governments and private entities for use in actual electronic data sharing pilot projects.
- Lessons learned from the pilot project were documented, and agreements were edited or augmented based on the experience of the pilots.
- Additional vetting and endorsements of the agreements were obtained from outside agencies, as noted in the final section of this document.

Policy Decisions and Guiding Principles

- The template agreements were drafted for use across all jurisdictions.
- HIPAA compliance was a guiding principle as part of an overall concern for privacy and security in eHIE.
- Agreements pertain to information requested only for the purposes of treatment, payment, health care operations, and, in the case of the public-to-public agreement, public health data.
- Specific categories of sensitive data, such as HIV and mental health information, are subject to state law and are not specifically addressed in these agreements.
- Each party would only share information that can be shared without additional specific protections.
- Each party will operate under and comply with its own applicable state law.
- Detailed provisions and technological specifications for user authentication, auditing, access, and authorization are not included in the templates. They are left to attachments agreed to by all parties.
- Each party's applicable state law will govern disputes, and in the event that a dispute cannot be resolved, the parties will look to federal law and the growing body of federal common law.
- Participation is voluntary and can be terminated at will. The IOA elected not to include governance provisions, as such provisions would limit the generality of the documents.
- Entering into these agreements does not change ownership of data.

Guidelines for Completing the Public Health Agreement

The Public Health Agreement is provided as a template. Further information needs to be inserted by parties to each agreement as follows:

- Effective date;
- Parties;
- Public health agency;
- State/territory;
- Public health system names (data registry names);
- Notice names and addresses;
- Signature information (name, title, date); and
- Attachments, as applicable, based on the parties' chosen structure for exchange and addition of parties (confidentiality agreement, timely delivery of information, standards, technological, and security specifications, etc.).

Additional Considerations for the Public Health Agreement

- The agreements will require additional attachments drafted by the users in the areas of technological specifications and timeliness of data exchange. See Section 3.0a. and 3.0c.iii. of the Public Health-to-Public Health Data Sharing Agreement.

- There are many public health exchange scenarios applicable to this agreement. To date, the IOA states have successfully used this agreement for immunization registry exchange.

- It is planned that this agreement will be expanded for additional uses in the future.

- Based on the experience of the IOA states, it is recommended that certain parties be involved in the review of these agreements in the early stages of a data sharing project. These organizations may include the state attorney general's office, governor's office, senior management of the Department of Public Health, registry program directors, technical staff, and Centers for Disease Control and Prevention (CDC) officials in each state.

Endorsements and/or Review of the Public Health Agreement

- American Immunization Registry Association (AIRA)

  During HISPC Phase III, the IOA Collaborative approached AIRA for its review and comment on the Public Health Data Sharing Agreement since the document was being used in the Iowa/South Dakota/Guam/New Jersey pilot electronic data sharing of live immunization data between the four members.

  The IOA Collaborative and AIRA had a number of very cordial calls and e-mails to discuss changes that AIRA suggested. The changes converted the IOA Public Health Data Sharing Agreement from a model document used in a pilot demonstration into a document that could be used for ongoing, continuing work among two or more public health registries. The suggested and accepted changes did not change the IOA Public Health Data Sharing Agreement in any substantive way.

  The AIRA endorsement letter dated January 2009 stated that the IOA Public Health Agreement is "formally endorsed by AIRA for use by all states and public health agencies for the interoperable exchange of public health immunization data."

  AIRA has loaded the updated version of the public health DSA to their website http://www.immregistries.org/ for download and use by their members.

- Public Health Data Standards Consortium (PHDSC)

  The PHDSC, established in July 2003, is a nonprofit membership-based organization of federal, state, and local health agencies; professional associations; academia; public and private sector organizations; international members; and individuals.

PHDSC's goal is to empower the health care and public health communities with health information technology (health IT) standards to improve individual and community health.

On February 18, 2009, the Board of Directors of the PHDSC approved the endorsement of the Public Health Data Sharing Agreement model document that had been developed and tested during the HISPC Phase III project.

They stated that the availability of this model agreement will greatly simplify the establishment of much-needed health information exchanges between public agencies across state lines, such as the sharing of immunization information between states from immunization registries. They look forward to working with the IOA Collaborative to advance the adoption and use of this agreement.

The PHDSC stated as part of its endorsement in February 2009 that "the availability of this model agreement will greatly simplify the establishment of much-needed health information exchanges between public agencies across state lines."

- Kansas

  In the fall of 2008, the State of Kansas approached the IOA Collaborative asking if it could review the Public Health Data Sharing Agreement. The IOA Collaborative agreed, and Kansas offered the following comments to the IOA Collaborative.

  Kansas felt that the Data Sharing Agreement is too formal for sharing within Kansas "for the purposes of sharing data . . . among agencies . . . to support our Community Health Record pilot project to get immunization and lead screening data" as the state has "good pre-existing relationships and data sharing agreements in place for related projects."

  Kansas did state that when the state does "embark on a statewide electronic record initiative in the future" that the IOA document will assist them. Kansas will use the provisions within the Public Health Data Sharing Agreement as a foundation tool when it takes this important statewide step.

- IOA Collaborative Public Health Pilot

  Iowa, South Dakota, Guam, and New Jersey signed the Public Health Data Sharing Agreement.

  The pilot-testing phase began after the model agreements were finalized halfway through the HISPC Phase III contract period. Pilot HIE project applications involved two or more states. The multistate HIE pilot projects included:

  - Iowa and South Dakota conducted a public health-to-public health Immunization Registry Exchange Project. This pilot project exchanged the immunization registry

data of those individuals 0–25 years of age who received treatment in bordering Iowa and South Dakota counties.

- Iowa, South Dakota, Guam, and New Jersey conducted a four-way public health-to-public health Immunization Registry Exchange Project. This pilot project exchanged the immunization registry data of individuals born in 1990. This population represents a geographically mobile group of 18-year-olds that includes both college- and military-bound individuals.
- New Jersey undertook several initiatives to promote and advance the mission of the IOA Collaborative and to expand the acceptance and use of the IOA Public Health Data Sharing Agreements. These activities included:
  - Meetings with New York State and City health IT officials to establish interstate exchanges of Immunization Registry data.
  - Meetings with the City of Philadelphia Department of Health and CDC officials to promote interstate exchange of Public Health Registry data.
  - Developed contacts with the Commonwealth of Pennsylvania Health Department for support in the New Jersey-Philadelphia immunization data exchange and for future data sharing opportunities with New Jersey.
  - Presentations to HIMSS, NGA, PAeHI and SLHIE on Public Health Data Sharing Agreements and the ability to share public health information data.
  - IOA representatives participated in two PA e-Health Initiative All-Committee Meetings and promoted HISPC initiatives to the group. A director from the committee attended the HISPC National Conference in Bethesda, MD, in March 2009.
  - Integration of DSAs into New Jersey's Electronic Medical Record exchange pilot project.

Frequently Asked Questions (FAQs)

HISPC Interorganizational Agreements (IOA) Collaborative
Model Data Sharing Agreements (DSAs)

Frequently Asked Questions (FAQs)

1. What is HISPC?

   Established in June 2006 by RTI International through a contract with the U.S. Department of Health and Human Services (HHS), the Health Information Security and Privacy Collaboration (HISPC) originally comprised 34 states and territories. Phase III of HISPC began in April 2008, comprising 42 states and territories, and aimed to address the privacy and security variations and challenges presented by electronic health information exchange (eHIE) through multistate collaboration.

2. What is the HISPC-IOA?

   In HISPC Phase III, participants were split into seven privacy and security topics for collaborative work, one of which was the IOA Collaborative.

   The IOA Collaborative included representatives from Alaska, Guam, Iowa, New Jersey, North Carolina, and South Dakota.

   Early phases of HISPC recognized that efforts to draft eHIE agreements and legal language can be time consuming and inefficient and often present barriers to eHIE. As a result, the IOA Collaborative proposed to develop and pilot test model DSAs. The stated objectives were to:

   - Develop a standardized set of model DSAs for eHIE focused on privacy and security; and
   - Test use of the model agreements in actual data-sharing pilot projects across state lines.

   The IOA Collaborative limited the scope of the project to two types of DSAs:

   1. Public health data exchange (“public-to-public” agreement); and
   2. Private entity data exchange (“private-to-private” agreement).

3. What is the mission of the HISPC-IOA?

   The mission of the HISPC-IOA is to improve patient care and safety by developing and implementing model DSAs to facilitate inter- and intrastate eHIE.

The project outcome is a set of model DSAs and related tools that can be shared nationally and replicated to advance eHIE efforts.

4. What was the general process used by the HISPC-IOA Collaborative?

   Through the use of HISPC-IOA legal Work Groups, the members of this collaborative reviewed a wide variety of memoranda of understandings, DSAs, and federal and state laws and regulations to develop consensus on core content and language. The Collaborative also coordinated with key groups, such as the Nationwide Health Information Network (NHIN) Data Use and Reciprocal Support Agreement (DURSA) Work Group and the other HISPC multistate collaboratives, to ensure consistency and continuity of effort.

   The IOA Collaborative documented a core set of privacy and security provisions and pilot tested the two model DSAs in real-life settings. Lessons learned from the pilots were used to create Implementation User Guides. Lastly, the IOA Collaborative requested additional review and feedback of the DSAs from various external organizations and agencies.

5. What are the primary product(s) of the IOA Collaborative work?

   - Two model DSAs: one for the public health setting and one for the private entity setting
   - Core privacy and security contract provisions
   - Implementation User Guides for the model DSAs
   - Library of sample DSAs
   - Compare/contrast analysis of the IOA model DSAs to the NHIN DURSA
   - Pilot evaluation results and formal approval/endorsements of the IOA model DSAs

6. Why should my organization use the HISPC-IOA model DSA(s)?

   The IOA Collaborative developed products for replication by other states and organizations to avoid duplication of effort. The IOA Collaborative took on this challenge so that organizations interested in eHIE would not have to go through a similar process and begin from scratch. We expect others to benefit from having access to standardized, endorsed DSAs that have been tested in real-life scenarios. Public health agencies and private health care entities can have confidence that the privacy and security aspects of the DSAs were thoroughly reviewed and vetted by experts in the field. Successes and barriers were documented to streamline future efforts. By providing template DSAs that can be easily customized, the IOA Collaborative aimed to create

momentum toward utilization of standardized documents throughout the country that will in turn encourage increased health information exchange.

7. How does one use the HISPC-IOA model DSAs?

   An organization should review the IOA model DSA templates and the respective Implementation User Guides with legal, medical, technical, and administrative representatives. The DSA templates provide a core model legal document. These templates can be modified, if necessary, through attachments to the core document to meet a specific organization's legal, medical, and/or business needs.

8. My organization already has a DSA or memorandum of understanding (MOU) for such activities. Why should my organization consider using the HISPC-IOA models?

   The HISPC-IOA is not advocating changes to current legal agreements that are already in place and used successfully to support eHIE. The HISPC-IOA model DSAs should be considered for new eHIE projects that will require new agreements or for existing agreements that need to be updated. By using the HISPC-IOA model agreements, many hours of administrative and legal time will be saved.

9. Should IT technical details and/or specifications be included in the HISPC-IOA model DSA?

   No. The HISPC-IOA model DSA templates are broadly worded to cover general areas of a DSA, with a special focus on privacy and security. Project specifics, such as IT technical details, should be drafted and attached as an appendix to the core document that can be easily modified as the project evolves. This accommodates the fact that technology changes more rapidly than the broader privacy and security provisions contained in the core document. Appendices such as IT technical details should, however, support the basic privacy and security concepts in the HISPC-IOA core documents.

10. What information is contained the Implementation User Guide?

    The Implementation User Guide is a companion resource for the model IOA DSAs that provides more explanation about the background, context, and use of the DSAs. The guides include such topics as policy decisions and guiding principles and user considerations for completing the DSAs.

11. Have the HISPC-IOA DSAs been pilot tested in real-life settings? If so, what organizations were involved in the pilots?

    Yes. Once the model templates were established, the agreements were pilot tested to assess their application in real eHIE projects. The pilot testing occurred in both the public health and private entity settings. Actual immunization registry data was exchanged between Guam, South Dakota, Iowa, and New Jersey as part of the public health pilot project. Preliminary approval of the agreements for future exchanges was obtained by 17

organizations in North Carolina and Alaska through the private pilot project. Using both public and private entities helped validate and increase trust in the agreements for future data sharing projects.

12. Is there a contact(s) that I can communicate with regarding the model DSAs? Legal details? Technical details? Etc.?

    Yes. The contact information is as follows:

    Alaska
    Rebecca Madison, Project Manager
    Alaska e-Health Network
    Phone: 907.729.3934
    e-mail: ramadison@anthc.org

    Guam
    Doris Crisostomo, Project Manager
    Office of the Governor of Guam
    Phone: 671.475.9380
    e-mail: healthyguam@gmail.com

    Iowa
    Susan Brown, Project Manager
    Iowa Foundation for Medical Care
    Phone: 515.440.8215
    e-mail: sbrown@ifmc.org

    New Jersey
    William O'Byrne, JD, Project Manager
    New Jersey Department of Banking and Insurance
    Phone: 609.292.5316, ext. 50032
    e-mail: wobyrne@dobi.state.nj.us

    North Carolina
    Roy Wyman, Jr., JD, Primary Contact
    Williams Mullen
    Phone: 919.981.4313
    e-mail: rwyman@williamsmullen.com

    South Dakota
    Kevin DeWald, Project Manager
    South Dakota Department of Health
    Phone 605.773.3361
    e-mail: Kevin.dewald@state.sd.us

13. Where can I find the final project documents for the HISPC-IOA Collaborative?

    HISPC-IOA deliverables will be publically available on the Office of the National Coordinator for Health Information Technology (ONC) website. Interested parties can also contact one of the IOA members from the listing above.

    Final project documents will be included in the HISPC-IOA Final Report and Appendices, March 2009.

    Appendices:

    - Model DSAs for Public Health Exchange and Private Entity Exchange
    - Implementation User Guide
    - Library of Data Sharing Agreements
    - Document Classification Scheme

- Core Privacy and Security Provisions for an Electronic Health Data Sharing Agreement
- NHIN DURSA Crosswalk Comparison with IOA Agreements

14. What organizations have approved or endorsed the HISPC-IOA DSAs?

    As of March 2009, the following organizations have approved or endorsed the HISPC-IOA DSA public-to-public model template:

    - Iowa Department of Public Health, October 2008
    - South Dakota Department of Health, November 2008
    - Guam, Office of the Governor, November 2008
    - American Immunization Registry Association (AIRA), January 2009
    - Public Health Data Standards Consortium (PHDSC), February 2009
    - New Jersey Department of Health, February 2009

15. Does this agreement apply only to the exchange of *electronic* health information?

    No. The HISPC-IOA DSAs can be adapted for any form of health information exchange, including paper-based exchanges. The same principles and high standards regarding the privacy and security of health care information should be applied to any mode of health information exchange.