APPENDIX H.
USER GUIDE: PRIVATE ENTITY DATA SHARING AGREEMENT

User Guide

HISPC Interorganizational Agreement (IOA) for Electronic Health Information Exchange

Private Entity-to-Private Entity 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 private-to-private data sharing agreement (Private Agreement) and explains the background, rationale, and other considerations related to use of the Private Agreement.

Background 2
Mission 2
Development Steps 3
Policy Decisions and Guiding Principles 4
Guidelines for Completing the Private Agreement 4
Additional Considerations for the Private Agreement 5
Frequently Asked Questions (FAQs) 7

[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 Private Agreement. A companion User Guide similarly addresses the Public Health-to-Public Health 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 public health entity ePHI exchanges is found in the Public Health-to-Public Health Data Sharing Agreement User Guide, which is a companion to the Public Health Data Sharing Agreement.*

2. Private entity-to-private entity exchange of PHI among private entities, such as between hospitals, medical centers, regional health information organizations, laboratories,

---

[2] "States" shall mean states and territories throughout this User Guide.

[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.

payors, PHRs, and other private organizations. *Information specific to the Private Agreement begins with the section "Guidelines for Completing the Private Agreement" below.*

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.
- The 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 extensively addressed in these agreements.
- Each party will 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.
- Additional parties may be added to the Private Agreement if the existing parties so decide. Alternative language is provided that sets out methods for such addition of parties.

Guidelines for Completing the Private Agreement

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

- Effective date;
- Parties;
- Type of entity;
- State/territory;
- Address;
- Exhibit numbers including the exhibit listing notice names and addresses;
- Number of days for deemed delivery;

- Alternative language for addition of parties (i.e., selection of the appropriate alternative and insertion of any necessary information);
- Signature information (name, title, date);
- 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.); and
- Nondiscrimination and other provisions that may be necessary under state law.

Additional Considerations for the Private Agreement[5]

- There are several attachments that may be beneficial to commence eHIE through the Private Agreement. Each attachment is described in footnotes to the Private Agreement, and it is ultimately up to the parties whether the attachments are necessary for the eHIE to meet each organization's individual standards. If the parties determine that a specific attachment is not necessary, the reference to such attachment should be removed from the agreement.

- There are also specific definitions or provisions that may be expanded or restricted based on the reason for eHIE between the parties. For example, providers may choose to expand the uses and disclosures to include research purposes. This is noted in the footnote to the "Permitted Uses and Disclosures" section, but the parties should review other sections of the agreement to determine whether additional revisions are necessary as a result of the nature of the individual agreement.

- The Private Agreement addresses proprietary information separately from protected health information, although both types of information are protected under the agreement. The agreement was drafted in this way to allow parties to place additional restrictions on proprietary information that would not ordinarily be exchanged if the parties continued to exchange records only in paper or hard-copy format. Protected health information is included within the definition of proprietary information in order to make clear that any breach of the proprietary information provisions using protected health information are in violation of the relevant provisions as well as, potentially, other provisions.

- Under HIPAA, individuals may request additional restrictions on the use and disclosure of information, and additional restrictions may apply under state or federal law. As described in Section 3c. of the Private Agreement, persons providing Protected Information should not rely on the receiving party to comply with any restrictions associated with the Protected Information. If the parties expand the exchange to include restricted information (whether it be restricted by state or federal law, such as HIV or substance abuse treatment information, or restricted by the individual, such as limits on access), specific procedures will need to be drafted as an attachment to the agreement to avoid violating those restrictions. The Private Agreement was structured in this way to

[5] Some areas for consideration are directly addressed in the footnotes to the Private Agreement and require no further elaboration. Parties utilizing the Private Agreement should review those footnotes while finalizing their own agreement.

avoid the difficulties that accompany the receipt of restricted information and create a barrier to the exchange of eHIE.

- The Participant Requirements laid out in Section 4 of the Private Agreement provide general requirements for access, monitoring, auditing, and other security processes. Depending on the sophistication of the parties, the standards attachment described in footnote 7 to the agreement may need to address any or all of the Participant Requirements, not just the access, use, and disclosure of Protected Information. The same applies to the Privacy and Security Safeguards described in Section 5 of the Private Agreement.

- As described in Section 7, "Warranties and Limitation of Liability," the Private Agreement does not shift the liability for use of Protected Information or actions taken based on the Protected Information. For this reason, it should not require additional insurance, though the parties should confirm with their insurance companies that any existing insurance will remain in full force and effect, as required by Section 10.

- The IOA determined for a variety of reasons that it should not include provisions for indemnification. We remained concerned, however, that a party might lack full protection in the event that an entity not a party to the contract harms a party to the contract with whom there is no privity of contract. We therefore drafted a provision to allow such a harmed party to bring suit against the entity causing the harm as though the harmed party were the party to the agreement that has such privity.

- The Private Agreement provides three alternatives for Section 14, addressing amendments and additional parties. These alternatives are explained in the footnotes to the agreement. Once the parties agree upon one of the alternatives, the other two alternatives should be deleted from the agreement.

- After the Private Agreement is executed, the parties should take steps to educate their Authorized Users about any applicable restrictions, standards, or procedures agreed upon by the parties to avoid additional liability. It may be beneficial to include this information in the organization's compliance plan, medical staff rules, or employee handbook.

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.