



# Health Information Privacy and Security Collaboration



## *Interstate Compact Innovation Task*

### **Overview of Task**

#### **1. Goal/Product and Purpose of the Interstate Compact Innovation Task:**

- To establish a foundational body of knowledge on the concepts that should be included, or considered for inclusion, in an interstate compact addressing consent in the context of electronic health information exchange.

#### **2. The collaborative will:**

- Identify and define potential elements and areas for consideration, including the purpose of each element or component.
- Identify various approaches to each element or component, as well as the implications and pros/cons (benefits/risks) of each approach.
- Identify potential challenges and provide analysis related to the feasibility of proposed approaches.

#### **3. The collaborative will not:**

- Make any recommendations or advocate for a particular approach/method.

### **Assumptions**

1. Due to the limited time available for the extension project, the specific language for each component of the Compact will not be developed.
2. Each component of the Compact will be researched to identify potential approaches and inform future development of the specific language of the Compact.
3. For clarification purposes, the “Requesting State” is the location where the original request for information is generated. The “Responding State” is the location where the request is received and a reply/action is taken based on the request.
4. An Interstate Compact may be enacted without formal consent of Congress, although Congressional approval may be required if the Compact involves potential federal authority.
5. The intent of the Compact is to:
  - a. Improve access to electronic patient information for permissible purposes where conflicting state laws may impede timely exchange.
  - b. Provide legal protection to Responding States if their laws are more stringent than the laws of the Requesting States.
  - c. Provide an option for states to adopt regarding consent that will preempt inconsistent state laws and therefore not require states to amend their existing laws.

*Interstate Compact Development Template*

<b>Component, Element, or Area for Consideration:</b> Certification for Data Privacy and Security to Support Interoperable Health Information Systems.	
<b>Summary of Various Approaches:</b> There are two primary options to consider when determining security policy for interstate health information exchange, and these are (1) using the existing HIPAA security provisions (2) developing or adopting a security standard. With either of these options an additional certification mechanism and insurance to cover the cost of data breaches.	
<b>1. Use HIPAA Security Rule and HITECH Enhancements</b> <ul style="list-style-type: none"> <li>• Require out-of-state receiving party to comply with HIPAA Privacy and Security Rules and HITECH enhancements.</li> <li>• Create certification process which allows disclosing entity to rely on certification rather than evaluating the receiving entity’s data privacy and security posture.</li> <li>• Establish insurance program that would cover costs of data breaches.</li> <li>• This option is the existing model for data protection today – with the exception of the certification and insurance components.</li> </ul>	<b>2. Develop a Data Privacy and Security Standard</b> <ul style="list-style-type: none"> <li>• Form an inter-state committee to review existing data privacy and security standards and develop a new standard for interstate data transfers.</li> <li>• Create certification process which allows disclosing entity to rely on certification rather than evaluating the receiving entity’s data privacy and security posture.</li> <li>• Establish insurance program that would cover costs of data breaches.</li> <li>• This option is not in place today.</li> </ul>
<b>Implications, Pros/Cons, Benefits/Risks of Each Approach:</b> The implications of the two approaches focus on the level of effort that will be required to comply with either approach. The primary drawbacks to the first option (HIPAA Security) are that current practices are variable (not scalable) and choice of law for interstate issues is not defined. The primary drawback to the second option (standard development/adoption) is that additional work is required. The issue with scalability can be best addressed with the standards development option because it would provide a well defined minimum requirement. The committee will need to address a standard for policies as well as technical implementations. <p>Another implication is that Option 1 (HIPAA Security) has been in place for a number of years and will continue to be updated and improved by federal regulators. On the other hand, Option 2 (standard development/adoption) may be difficult to draft because, on a practical level, state representatives on the committee may not easily or rapidly agree on another security standard.</p>	
<u>Pros:</u>	<u>Pros:</u>

Formatted: Indent: Left: 0.13"

<p>1. Use of the HIPAA Security Rule and HITECH enhancements</p> <ul style="list-style-type: none"> <li>• allows more flexibility for receiving entities to develop data privacy and security programs commensurate with their specific risks.</li> <li>• simplifies compliance by allowing the receiving entities to monitor changes in one set of requirements.</li> <li>• allows receiving entities to comply with one data privacy and security rule.</li> <li>• can be enforced by state AGs, who have been granted authority to enforce HIPAA per the HITECH Act.</li> </ul> <p>2. The certification process makes it easier to share data because the disclosing party can share information with the understanding that the receiving party has adequate controls in place to protect the information.</p> <p>3. The insurance component supports the sharing of information by socializing the breach notification costs across all entities participating in data transfers. Insurance revenues could help subsidize certification process.</p> <p><u>Cons:</u></p> <p>1. Use of the HIPAA Security Rule and HITECH enhancements</p> <ul style="list-style-type: none"> <li>• may not be equal among different types and sizes of entities because the risk analysis is scalable.</li> <li>• may not account for state-specific data privacy and security laws that are more stringent.</li> <li>• are not very proscriptive, at least yet. Receiving entities may choose to implement lax data privacy and security standards.</li> <li>• may need to also include the HIPAA Privacy Rule, which may be difficult to</li> </ul>	<p>1. Developing a Data Privacy and Security Standard</p> <ul style="list-style-type: none"> <li>• facilitates the creation of a new data privacy and security standard that accounts for state-specific data protection requirements.</li> <li>• allows states to create a more proscriptive approach to data privacy and security.</li> <li>• allows those states participating in the compact to create a safe harbor for compliance with state data privacy and security laws.</li> <li>• leverages the work that has been done in various arenas, such as the Uniform Security Standard and the Data Use and Reciprocal Support Agreement and the Uniform Security Policy.</li> </ul> <p>2. The certification process makes it easier to share data because the disclosing party can share information with the understanding that the receiving party has adequate controls in place to protect the information.</p> <p>3. The insurance component supports the sharing of information by socializing the breach notification costs across all entities participating in data transfers. Insurance revenues could help subsidize certification process.</p> <p><u>Cons:</u></p> <p>1. Developing a new data privacy and security standard</p> <ul style="list-style-type: none"> <li>• is a duplicative effort that steers resources away from other aspects of managing interstate data transfers.</li> <li>• adds another regulation that receiving entities must monitor, analyze, and implement.</li> <li>• requires the development of a new enforcement mechanism.</li> </ul> <p>2. The certification and insurance programs have not been developed and the administration of these programs may</p>
--	---

<p>operationalize because the receiving entity may not be conducting a HIPAA-covered function for the disclosing entity.</p> <ul style="list-style-type: none"> <li>• have yet to be drafted and analyzed for effectiveness and feasibility of implementation.</li> <li>• requires discussion regarding choice of state venue.</li> </ul> <p>2. The certification and insurance programs have not been developed and the administration of these programs may pose additional difficulties.</p>	<p>pose additional difficulties.</p>
<p><b>Potential Challenges and Analysis of Feasibility of Each Approach:</b> Challenges focus on the clarity of requirements in either option and the amount of effort to achieve this clarity.</p>	
<p>a. Challenges to using HIPAA Security Rule and HITECH Enhancements</p> <ul style="list-style-type: none"> <li>• Variations in state law and choice of law are problematic</li> <li>• Certification is a challenge in either scenario</li> <li>• Insurance is a challenge in either scenario</li> <li>• Large and small entities do not have standard safeguards and mitigations for risk; scalability is an issue</li> </ul> <p>b. Feasibility of using HIPAA Security Rule and HITECH Enhancements</p> <ul style="list-style-type: none"> <li>• Dependent on federal regulation and interpretation</li> <li>• Enforcement may vary by state AG resources</li> </ul>	<p>c. Challenges to Develop a Data Privacy and Security Standard</p> <ul style="list-style-type: none"> <li>• New processes are onerous</li> <li>• Standards development is usually a technical issue not a policy issue</li> <li>• Certification is a challenge in either scenario</li> <li>• Insurance is a challenge in either scenario</li> <li>• Enforcement may be an issue</li> </ul> <p>d. Feasibility to Develop a Data Privacy and Security Standard</p> <ul style="list-style-type: none"> <li>• Cost could be subsidized by insurance</li> <li>• Utility and pay off is long term</li> </ul>
<p><b>Comments:</b> (Includes any comments that would be instructive or helpful as background or to provide a context for evaluating the various approaches that could be considered).  <b>The Uniform Security Policy (USP) for health information exchange among states has been completed for two of four security domains under other HISPC work.</b></p>	
<p><b>References:</b></p>	
<p>HIPAA HITECH Act</p>	<p>DURSA USP</p>