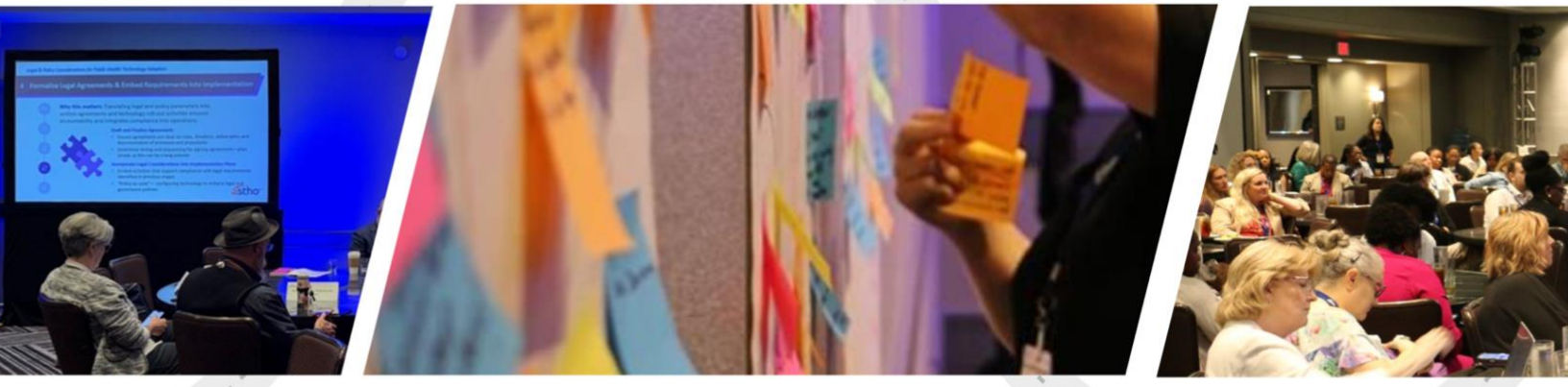
ASTHOReport

Legal and Policy Considerations for Public Health Technology Adoption: An Exploratory Guide



July 2025

Acknowledgments

ASTHO would like to thank CDC for their support and input on this project, in addition to ChangeLab Solutions for their contributions. This exploratory guide also benefited from the practice-based experiences of state and territorial health agency leaders, without whom this work would not be possible.

Authors

Reema Mistry
Director, Public Health Data Modernization & Informatics
ASTHO

Elizabeth Ruebush
Senior Director, Public Health Data Modernization & Informatics
ASTHO

Andy-Baker White
Senior Director, State Health Policy
ASTHO

Wesley Hartman
Senior Attorney
ChangeLab Solutions

Erik Skinner
Senior Analyst, Public Health Data Modernization & Informatics
ASTHO

Lillian Colasurdo
Director, Public Health Law & Data Sharing
ASTHO

Contributors

Alexandra Woodward
Senior Advisor, Public Health Data Modernization & Informatics
ASTHO

Amanda Fernandes
Senior Attorney
ChangeLab Solutions

Jami Crespo
Senior Attorney
ChangeLab Solutions

Heidi Westermann
Director, Public Health Data Modernization & Informatics
ASTHO

This work was supported by the Strengthening Public Health Systems and Services Through National Partnerships to Improve and Protect the Nation's Health CDC-RFA-PW-24-0080 Cooperative Agreement, funded by the Centers for Disease Control and Prevention (CDC). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the Centers for Disease Control and Prevention. This report is not intended to serve as legal advice from the organizations that created this document, or from the funders of those organizations.

Introduction

An array of modern interoperability technologies and frameworks can support how public health agencies access, manage, use, and share data from multiple sources. Health agencies must consider many critical factors (e.g., legal and policy) when assessing, adopting, and implementing new technologies and interoperability solutions. These technology solutions may streamline data exchange, enhance data quality and access, and reduce manual burden on public health staff by supporting data collection, analysis, and reporting. While specific legal and policy considerations may vary based on the nature of the technology the health agency is adopting, intended use case(s), and jurisdictional context, there are common processes that can help assess technology from a legal and policy lens and recurring themes in the issues that are often explored.

About This Guide

This exploratory guide aims to help multidisciplinary teams identify legal and policy considerations as they assess and adopt new technologies, identify necessary agreements, and support compliance with legal requirements throughout the technology lifecycle. ASTHO developed this guide in collaboration with ChangeLab Solutions, with support from CDC. It incorporates information from a scan of secondary sources and input from state and territorial (S/T) public health leaders during an interactive session on legal considerations for interoperability technology adoption at ASTHO's Executive Leadership Forum and related meetings in June 2025.

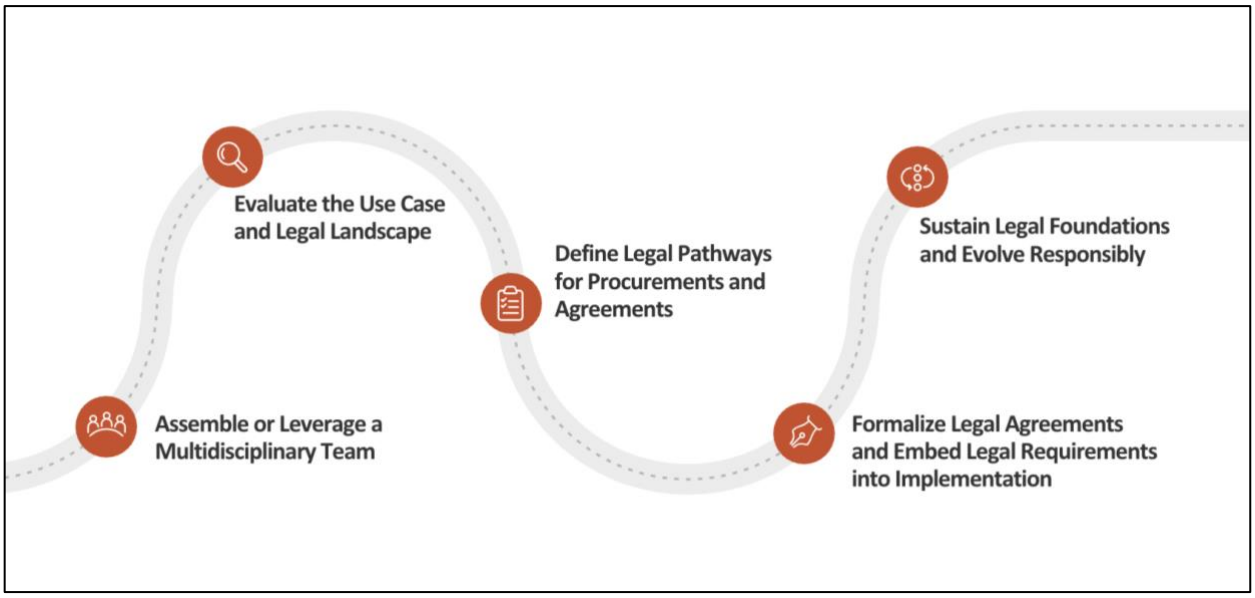
For clarity and usability, this guide is presented as a stepwise framework. In practice, however, the sequence of activities may depend on the jurisdiction's operating environment. Some activities may occur in parallel or may need to be revisited as circumstances evolve. Additionally, while this exploratory guide focuses on the legal and policy considerations involved in the adoption of *new* interoperability technologies and frameworks in public health settings, some of the considerations listed may also be relevant to enhancements, upgrades, or vendor transitions for existing systems. Finally, this document is framed as an exploratory guide, as continued and broader collection of implementation-based insights is essential for creating a comprehensive list of considerations.

Interoperability Technology Solutions and Frameworks

A variety of technology solutions and frameworks can support improved public health interoperability. Some examples include the following:

- **Data Integration Building Bocks (DIBBs)** offer modular, open-source tooling that can help clean, validate, and enrich data as it moves through health department workflows.[1]
- **The National Electronic Disease Surveillance System Base System (NBS)** is a CDC-developed information system that integrates data across multiple public health conditions and facilitates the management of reportable disease data and transmission of notifiable disease data to CDC.[2]
- **The Trusted Exchange Framework and Common Agreement (TEFCA)** aims to support nationwide health information exchange through network-based exchange.[3]

FIGURE 1 | Navigating Legal and Policy Considerations Associated with Public Health Interoperability Technology Adoption



1 | Assemble or Leverage an Existing Multidisciplinary Team

Given the interplay of programmatic, technical, and legal considerations that may inform decision-making around the adoption of a new public health interoperability technology, a multidisciplinary working group may be necessary to assess the implications of a new technology solution. This section includes information regarding core areas of expertise to engage in a multidisciplinary team, approaches for organizing the team's work, promising practices for working with legal counsel, and practice-based experiences from S/T health agency leaders.

Core Areas of Expertise

Programmatic staff, epidemiologists, and data stewards should be engaged in planning efforts to assess and adopt new interoperability technologies and frameworks. These roles can provide context around the public health goals and outcomes the technology will facilitate the data elements necessary for the intended use case; partners involved in data collection, exchange, and use of the data; and staff resources (e.g., training and other workforce development needs) that may facilitate effective use of the technology.

Informatics and technology expertise is also critical. Informaticians can support the effective use of information technologies for public health purposes and bring essential expertise in data standards. Consider engaging informatics and technology roles such as data modernization/informatics director, chief information officer, IT specialist, data governance officer, and information security officer.

Tip: You may not need to build a team from scratch. Consider leveraging existing cross-functional teams, such as data modernization advisory groups.

Informaticians often liaise between public program areas and IT department staff to ensure a shared understanding of programmatic needs and technology solutions to meet those needs.[4] IT department staff can support integration of a new technology solution within existing infrastructure, assess compatibility with current system capabilities, and address data security measures. In addition to managing day-to-day operational security controls (e.g., network access, password policies, etc.), IT departments may also have an information security officer or similar role, charged with monitoring technical safeguards, performing vulnerability assessments, and responding to security incidents.

Legal and compliance experts should also be engaged to assess and guide adoption of new interoperability technologies. Their role involves confirming that how data will be managed, accessed, used, and shared through the proposed technology align with relevant laws. S/T health agencies can offer legal counsel services through a variety of mechanisms, including contract with independent private attorney or law firm; external agency (e.g., Attorney General's office); attorney(s) that a specific bureau or group of agencies share; or dedicated in-house general counsel.[5] Public health attorneys' approaches to representation can vary from risk avoidance, seeking to minimize any potential liability for a client, to helping a client balance legal and public health considerations to achieve an important goal.[6] Engaging legal counsel early when exploring a new interoperability technology is recommended.

In addition to legal counsel, other staff may bring valuable legal and policy insights. For example, program staff may have direct knowledge of S/T laws relevant to their program's collection, sharing, and use of data. Other staff, such as compliance or privacy officers, may have formal legal training and support a variety of functions such as legal interpretation, policy development, and compliance. Together, staff with varying legal expertise can serve the following functions related to technology and interoperability:

- Reviewing policies and legal agreements.
- Drafting new policies or new language for legal agreements.
- Ensuring compliance with applicable laws and policies once technology is in use.
- Drafting governance documents.

Health agencies may also consider involving **operations staff**, who might support procurement processes and have insights related to timelines/procedures for acquiring and implementing new technologies.

Approaches for Organizing the Team's Work

Once a multidisciplinary team has assembled, it is important to clarify how the team will function and make decisions as they navigate complexities associated with assessing and potentially adopting a new interoperability technology. The team should define roles and responsibilities, establish clear decision-making authorities and processes, and set expectations around coordination. Aligning on these details is essential, as team members may originate from different departments with their own reporting structures, responsibilities, and established processes that may need to be respected.

Teams may benefit from establishing a regular meeting cadence and can also consider creating sub-groups to focus on specific areas of work. Setting ground rules for how to disseminate pre-work (e.g., review of draft agreements, data flow analyses) and expectations for review and/or feedback prior to meetings can help ensure smooth collaboration and progress towards goals. Progress may need to be reported to parties outside of the working group (i.e., within the health agency, or beyond, depending on the jurisdiction's governance structures). There may also be multiple decision-makers for different areas of expertise who need to provide approval to move forward with adoption of a new technology, such as an S/T health official, a state data or technology officer, and General Counsel. These leaders will need sufficient information regarding the public health, technology, and legal considerations to make informed decisions about the interoperability technology.

Notably, S/T governance structures may inform coordination approaches. IT and legal functions may be dedicated to the health agency or centralized at the state level. Only 51% of S/T health agencies directly oversee their IT functions within their department, while 56% directly oversee legal services and analysis functions.[7] The location where IT and legal functions are managed may impact both the flexibility and authority the health agency may have in making decisions to purchase, adopt, or connect to new technology systems and tools.

Promising Practices for Working with Legal Counsel

- **Ask directly, share fully:** Be clear in what you are asking but never selectively withhold information.
- **Set expectations:** Be honest and open about your goals including the why.
  - What's the use case?
  - What's the public health goal and importance?
  - What data elements are involved and how will the data be used?
  - What technology will be used?
- **Share what you know and ask what they need:** If you know relevant laws and/or have relevant documents, share them.
  - If you don't want to send too much, ask what would be helpful to send.
- **Engage early and flag key deadlines:** Be transparent about timelines and try to contact your attorney early in the process.

Insights From S/T Public Health Agency Leaders

Informatics experts, public health lawyers, and other health agency senior leaders shared the following:

- **Stay open-minded to technology solutions and establish more efficient review processes where possible:** The COVID-19 pandemic made an excellent case study for prioritized and expedited review of important public health technology-related decisions to make data readily accessible and usable. The mindsets, particularly of legal and compliance staff, shifted during this time, recognizing the importance of making decisions quickly. Nurturing a similar mindset — emphasizing the critical public health outcomes supported by a technology — for times when there isn't a public health emergency can help expedite technology review and decision processes.
- **Be transparent and engaged with all necessary partners early and often:** A regular cadence of meetings and well-established working relationships can help drive technology review and decision processes forward. Everyone should be prepared to share their own expertise and the information that they have with other parties involved.
- **Centralized administrative functions can pose a barrier, mitigated by dedicated public health representation:** For health agencies that do not directly oversee some of their own functions (e.g., relying on a centralized state IT office or centralized legal representation), working with these external partners can be a barrier. One way to support better technology review and decision policies is to have dedicated public health representation in these contexts.
- **Navigating multiple decision-making structures can present challenges:** While data governance, security, and compliance are interrelated, there can be a bifurcation in how these functions are structured. Identifying the lanes of work and areas of decision-making authority can be challenging. The need for coordination across many separate structures can also create bottlenecks in decision-making.

2 | Evaluate the Use Case and Legal Landscape

Once a multidisciplinary team is in place, the next stage of work involves evaluating the use case, technology solution, and legal landscape. This step helps ensure that proposed interoperability technologies are technically sound, appropriately governed, and legally permissible. This section outlines considerations for assessing the technology and use case, identifying applicable data and IT governance policies, and conducting a legal analysis.

Understand the Use Case and Technology

Implementation of a new interoperability technology often starts with a specific, limited use case. Preliminary review of the technology solution should consider specifics of this use case. When defining the use case, the multidisciplinary team should consider the data elements involved, how the data will be used, and with whom it will be shared. A data sharing legal framework from the Network for Public Health Law offers guidance on the "building blocks" for developing a use case and the value of creating a data flow map to characterize how data move through and across systems.

Exploring details about the technology solution itself — to understand how data are stored, accessed, encrypted, hosted, and audited within the technology environment — is critical at this stage, and can also help inform development of data flow maps. This stage of the process is also a good point to start reviewing contracts and service level agreements with a practical implementation-based lens. From this standpoint, contracts should include details regarding testing and validation procedures that might be required before full deployment of the technology.

Identify and Align with Applicable Data and IT Governance Policies

Data governance refers to internal standards, roles, processes, and policies that dictate data management, storage, integrity, security, sharing, and usage. IT governance complements data governance and refers to internal standards, roles, processes, and policies that dictate IT management, strategy, operations, and security.[8] Together, data and IT governance policies may influence approaches for assessing the "fitness" of a new technology within a health agency's existing organizational policies. Note that while this section addresses data and IT governance explicitly, governance considerations are cross-cutting, informing multiple stages in the technology assessment and adoption process.

Data governance can inform the data sharing agreements, operating policies and oversight processes[9] associated with adopting a new technology. Staff should assess the use case and technology against these governance policies to determine whether the proposed solution aligns with protocols, whether policies adequately address the questions and risks raised by implementation, and whether updates or clarifications to governance policies are needed to support responsible adoption. Technology adoption can expose gaps or inconsistencies in governance policies. Implementation of a new technology can be an opportunity to identify and address outdated or unclear policies.

Tip: Key questions to ask while assessing alignment between governance policies and technology adoption:

- Does adoption of a technology solution fit with the current governance policy?
- Are there gaps in governance policies related to this technology or use case?
- Is there a need for revision of outdated/unclear governance policies/protocols to support implementation?

Governance can also help inform what is "coded" into process. Specific requirements (e.g., data access permissions, data retention, and approvals for exporting data) can be translated into technical configurations. This reflects the concept of "policy as code," where governance policies can directly shape technology configuration and implementation, ultimately supporting compliance by aligning system behavior with policy expectations.

Finally, it is important to note that data and IT governance policies may be agency-wide or more limited in scope. Ideally, the multidisciplinary team should work to align technology use cases with existing governance structures, rather than creating siloed frameworks for specific technology implementation projects.

Identify Applicable Laws

Specific statutes, regulations, case law, and policies will impact adoption and implementation of the technology solution under consideration. Legal experts should assess which jurisdictional laws need to be considered, including data sovereignty rules, when applicable. Similarly, legal experts should explore whether there are jurisdictional laws that authorize, prohibit, or are simply not specific enough to allow the health agency to collect certain data fields that might be relevant to the identified use case.

Laws may also expressly delegate authority or may intentionally be written broadly, leaving policy choices and implementation up to public health and technology experts through sub-regulatory guidance/practice. In these cases, legal experts need to work closely with the multidisciplinary team to fully understand how laws might apply or be implemented.

Tip: Create a list of relevant laws, with input from legal, security, compliance, and program teams. The goal is to identify and address issues early in the process.

A health agency's Health Insurance Portability and Accountability Act (HIPAA) status may also impact legal considerations associated with a new interoperability technology adoption. See Appendix 1 for a primer on relevant HIPAA terms. Some technology solutions involve sharing data with the federal government; see Appendix 2 for a working list of federal laws that may come into play in these scenarios.

Following identification of relevant laws, the team should apply them to the use case and technology under consideration.[10] Guiding questions to consider, with the specific technology solution in mind, include the following:

- **What data can be shared?** Federal and jurisdictional laws may require or at least permit, specified data sharing. Federal and jurisdictional laws may have differing requirements around individually identifiable data, compared to non-identifiable, de-identified, or summary or aggregate data. There also may be differing requirements for specific populations or types of data, such as substance use and mental health data, HIV, or data about children.
- **With whom can data be shared?** Federal and jurisdictional laws may require, or permit, data sharing with specified partners.
- **For what purposes can data be shared or used?** The main purposes for data sharing, generally include indicators and reporting; analytics, research, and evaluation; and operations and service delivery.[11] Federal and jurisdictional laws may define specific public health purposes for which data can be used and may permit other secondary uses of public health data such as for research or potentially enforcement purposes.

When assessing legal risk associated with a new interoperability technology, health agencies should consider downstream data access and secondary use risks, evaluating the potential for further dissemination, repurposing, or re-identification of data. Agreements and safeguards can limit access and clarify permissible uses consistent with public health intent and legal requirements.

Insights From S/T Public Health Agency Leaders

Informatics experts, public health lawyers, and other health agency senior leaders shared the following:

- **Too much risk aversion can be a barrier, and risk aversion may compound other potential legal and policy barriers:** Risk aversion can impact every aspect of technology review and decision-making, and it can be applied across different expertise. For example, while attorneys may take a risk averse approach to legal compliance, IT staff can be equally risk averse to new technology. In particular, many involved in technology decisions may take a risk averse approach to compliance with privacy laws, such as HIPAA, Family Educational Rights and Privacy Act, or 42 CFR Part 2, which protects confidentiality of records of patients with substance use disorder. Ways to navigate this particular type of risk aversion include reliance on other laws and policies that underscore permissiveness of technology use and data sharing, such as the information blocking provision of the 21st Century Cures Act, as well as more affirmative framing: "Why wouldn't we use interoperability technology?" instead of, "Why would we use interoperability technology?"
- **Pilot with an initial, limited use case, but consider future use cases from the beginning:** A health agency's use of technology needs to serve a purpose. For new technology, or new uses of technology, a specific use case needs to be articulated that justifies its adoption. However, review and decision-making should consider potential future use cases, to avoid establishing unneeded constraints limiting reasonable use of the technology. While it may be helpful to articulate a limited, single use case for purposes of first adopting and implementing a technology, be sure to build in planned future use cases and recognize how the technology connects to all existing systems and processes.
- **Legal assessments should consider primary and secondary uses of data:** These uses should be called out explicitly in any agreements that are developed. Downstream, secondary uses of public health data frequently raise legal and policy issues, and legal and program staff and/or technology providers may have different perspectives on secondary uses of data. Some secondary uses could require Institutional Review Board review or other approvals.
- **Tools to support security and legal review of new technologies would be beneficial:** Best practice frameworks, checklists, and risk assessment guides would be helpful in supporting health agencies as they assess and adopt new interoperability technologies.

3 | Define Legal Pathways for Procurement and Agreements

As health agencies define a use case and review applicable federal and jurisdictional laws, establishing a clear, shared understanding of the procurement rules and necessary legal agreements early on can help prevent delays and lay a solid legal foundation for smooth implementation. This section outlines key considerations for selecting a vendor, including industry-standard certifications, types of legal agreements, and aligning decision-making with the multidisciplinary team.

Identify Rules Associated with Vendor Procurement

When adopting a technology solution that involves a third-party vendor, it is important to consider relevant jurisdictional laws and procurement policies. These requirements may mandate competitive bid solicitation, require specific justifications for sole-source contracting, or define vendor eligibility considerations. If considering a cloud-based solution, for example, health agencies must ensure that the vendor holds the necessary certifications, such as FedRAMP[12] or GovRAMP,[13] which demonstrate compliance with federal or state privacy, security, and data standards for cloud security. These certifications are critical in confirming that the vendor's products meet the required regulatory standards. Understanding these policies early in the process helps ensure compliance and avoid delays.

Health agencies should request relevant compliance certifications, reports, and security protocols to verify that their technology solution aligns with the procurement needs of the health agency. Thoroughly reviewing vendor contracts and service-level agreements (SLAs) is also vital to ensure that all terms are clearly defined and that the vendor can deliver the expected level of service and support.

Identify Agreements Needed for Implementation

Jurisdictional laws may require specific types of legal agreements, such as data use agreements, when procuring technology solutions from vendors, or when entering into an interoperability agreement with another entity by means of the technology solution. These agreements help ensure that the technologies and data are used in compliance with relevant laws and policies. The multidisciplinary team should identify the agreements needed to advance technology implementation early, to allow sufficient time for negotiation and approval of agreement language.

Types of agreements that may be needed to implement a new interoperability technology include:

- **Vendor or service provider contracts:** Legally binding agreements between an agency and a vendor or service provider that outlines the terms and conditions for services or goods. The obligations, responsibilities, and expectations of both parties involved in the contractual relationship are set out in the agreement.
- **Data sharing agreements and data use agreements (DSAs and DUAs):** Legally enforceable agreements that set out the terms and conditions for using or sharing data. These agreements state the legal authority for the data sharing and use, specify the purpose and permitted uses of the data, identify the data elements that are shared, often provide how the data will be kept safe and secure, and can describe methods for monitoring and ensuring compliance with the agreement.
- **Memorandum of understanding:** These agreements are non-binding and offer fewer legal protections than data sharing agreements or data use agreements. They often outline the scope, details, and terms between the parties as well as each party's roles and responsibilities.
- **Business associate agreements (BAAs):** HIPAA requires covered entities to enter into BAAs with their business associates (i.e., a person or entity who provides certain services to a covered entity and who is allowed access to protected health information). These agreements help ensure that the business associate properly safeguards protected health information and that any data is used or disclosed only as allowed or required by contract or law.
- **Other structured agreements** that outline how data is to be shared, handled, accessed, retained, destroyed, and/or returned.

Develop a Legal/Policy Recommendation

Based on aforementioned legal and policy assessment activities, a determination should be made regarding the feasibility of moving forward with adopting the new technology. This recommendation should be accompanied by input from informatics/IT and programmatic experts, who similarly would have assessed the feasibility of implementing the technology based on desired program goals and integration into existing data infrastructure. If the recommendation is to proceed with technology adoption, ensure that all relevant decision-makers identified earlier in the process are informed and have provided their approval.

Insights From S/T Public Health Agency Leaders

Informatics experts, public health lawyers, and other health agency senior leaders shared the following:

- **Procurement policies have been a significant barrier:** Similar to challenges with other centralized functions described earlier, some health agencies faced challenges working with external business development and procurement offices. Staff training and understanding of procurement processes can alleviate some of these barriers so staff are not learning the processes as they go through it. Others noted that procurement processes can be inefficient or unaligned with the reality of public health practice, such as requirements that every planned use case of a new technology be reviewed separately.
- **Obtain technology vendor terms and conditions early to avoid legal delays:** Vendor agreements usually have two components — the substance of agreement (i.e., language that covers information about the use case, data fields, etc.) and boilerplate terms and conditions language. This boilerplate language can include indemnification clauses and proprietary protections that can prolong legal reviews or revisions at health agencies. Boilerplate language can be disaggregated from other components of the agreement and submitted for legal review early in the process, which can help avoid bottlenecks or delays at later stages of agreement review and finalization.

4 | Formalize Legal Agreements and Embed Legal Requirements into Implementation

Once a decision has been made to adopt a technology solution, health agencies should translate legal and policy parameters into written agreements and implementation plans. This ensures accountability and integrates compliance into operations. This section outlines key considerations for drafting and finalizing legal agreements, and recommendations for translating policy into practice.

Draft and Finalize Legal Agreements

As a health agency decides to pursue the adoption of a technology solution, ideally with input and consensus from the multidisciplinary team, contractual and legal experts should draft appropriate agreements to move towards implementation. Agreements should be clear on roles, timelines, deliverables and documentation of all processes and procedures. They should also include data governance considerations such as data access control, retention policies, and privacy and security protocols.

Tip: The timing and sequencing of the agreements may depend on the type of agreements that need to be executed. Consider when agreements will need to be in place and allocate sufficient time for legal review and approval when planning.

Agreement negotiations can be lengthy, with opportunities for delay at multiple points of the process and across the multiple parties involved in review, revision, and execution. Health agencies should consider the timing of signing the agreements as entities may have their own templates or preferences for language in agreements that would need to be reconciled through an iterative process, which may add time to the implementation timeline.

Incorporate Policy Considerations into Implementation Plan

A technology implementation plan can serve as a roadmap that clearly outlines actions required to adopt a new technology solution. It can guide a multidisciplinary team from planning through execution by detailing key steps such as testing, validation, and data production. Additionally, the plan can incorporate activities and processes that support compliance with governance and legal requirements identified in the previous steps.

Opportunities to Incorporate Legal and Policy Considerations into Implementation Plans

- **Key roles and responsibilities** regarding oversight of activities required by policy or law.
- **Approaches for monitoring**, auditing, and ensuring compliance.
- **Protocols for data privacy and security**.
- **Staff training** on legal and compliance requirements associated with management and use of the new technology, including the deliverables or outcomes staff should monitor for from the agreements, and what they should do if those deliverables are not being met. Trainings should include a process for when and how to reach out to legal staff if/when significant performance issues arise, including if the vendor is in breach of their contractual obligations.

Insights From S/T Public Health Agency Leaders

Informatics experts, public health lawyers, and other health agency senior leaders shared the following:

- **A variety of barriers can arise when working with third-party vendors:** Health agencies noted challenges when technology use and adoption necessitates the use of third-party vendors. Vendors may find it difficult to meet heightened security requirements. They may also be hesitant to share documentation needed for health agencies to complete their review of a technology due to fear of state freedom of information, sunshine, or open records laws that could expose their proprietary systems and security measures to the potential for public disclosure. Additionally, if vendors employ overseas staff, they could fail to meet varying state security or privacy requirements.

5 | Sustain Legal Foundations and Evolve Responsibly

Use cases, technologies, and the policy landscape evolve over time, and it is good practice to establish norms around how a health agency will maintain interoperability technologies and related operations. As health agencies experience staff turnover, documenting maintenance plans and offering trainings can support continuity of compliance and oversight activities. This section outlines key considerations for establishing legal maintenance into ongoing operations, scaling use of technology, and maintaining cross-functional capacity.

Incorporate Policy Maintenance into Ongoing Operations

A technology maintenance plan can help plan for scheduled system updates and routine maintenance to ensure optimal performance. In addition to these standard components, a technology maintenance plan can build in a schedule for reviewing and renewing DUAs, BAAs, vendor contracts, and other agreements, to ensure these agreements do not lapse and impact continuity of the technology service. A maintenance plan may also include processes for ongoing technology compliance monitoring and auditing.

Sustaining Compliance in an Evolving Environment

Ensuring compliance is an ongoing process that must adapt to a variety of changing circumstances. Changes in data and IT governance policies, shifting leadership priorities, and updates to federal or jurisdictional regulations may all signal the need to reassess existing technology solutions. Maintaining compliance also requires regularly updating user permissions and conducting staff training that reflects current policy and procedures for use of the technology. Training is important in facilitating compliant process and procedure, especially in the face of policy and operational changes and staff turnover.

Scale Use Thoughtfully and with Cross-Functional Input

Interoperability technologies may be suitable for scaling to support additional use cases. Expanding use cases may require additional legal and data/IT governance review. Depending on the types of data, users, and entities involved in the expanded use case(s), the jurisdictional and federal laws may vary in their applicability and impact.

It is essential to engage a multidisciplinary team to guide decisions and maintain awareness about the expanded use of technology. Decisions related to evolving applications of the technology and/or policies may have downstream effects on other agency-wide functions such as informatics/IT, program, and legal compliance. Any decisions taken should be aligned with broader agency priorities. Over time, sustaining connections between informatics, program, and legal counsel can help ensure awareness of evolving policies and/or applications of the technology, and aligned decision-making.

Insights From S/T Public Health Agency Leaders

Informatics experts, public health lawyers, and other health agency senior leaders shared the following:

- **Changes, enhancements, or upgrades for existing products often means starting over.** Health agencies noted the challenges they experience when rolling out upgrades or expansions for existing technology tools. Often, the agency must begin or renew the entire approval or procurement process for what may be a slight change to the current technology, which already went through the lengthy process.

Conclusion

A legally sound infrastructure is essential for the successful implementation of public health technology solutions, which hold significant potential to enhance data sharing, accessibility, analysis, and reporting. S/T public health agency leaders noted that additional resources and technical assistance would be useful in helping them navigate policy considerations associated with new interoperability technologies. They highlighted templates and checklists to complement the steps outlined in this exploratory guide as useful tools — in particular, templates for use cases and checklists for legal and IT clearance processes. They also noted that the following assistance would be beneficial: support translating technical specifications to legal and procurement partners; frameworks and approaches for working in risk-averse environments; and comprehensive best practices guidance to address commonly encountered challenges. While this exploratory guide provides a foundational roadmap for agencies considering the adoption of new technologies, capturing practice-based experiences will be critical to refining and establishing effective, sustainable pathways forward.

APPENDIX 1

HIPAA and Data Privacy Primer

Who does HIPAA apply to? HIPAA applies to covered entities and business associates of covered entities.

What is a covered entity? Covered entities include health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form.

What is a business associate? Business associates are any person or organization outside of the covered entity that performs functions and activities on behalf of or for a covered entity *and* those functions, activities, or services require the use or disclosure of individually identifiable health information. If a covered entity wants to work with an outside person or organization, such as an IT vendor, and that work will require that they have access to or may view protected health information, that vendor must first sign a BAA.[14]

How does HIPAA apply to public health agencies? Many health agencies have programs that serve as health care providers (e.g., WIC clinics, immunization clinics, childhood developmental screening programs). A health department may decide to "hybridize" under HIPAA, which would section off those provider-type programs from the other general public health programs. Hybridization requires the department to undergo a thorough analysis and documentation process of how HIPAA does or does not apply to each program and may limit data sharing between programs.[15] Many jurisdictions have taken a different approach, and instead the entire agency is a covered entity under HIPAA, including general public health programs.

How does privacy and security relate to HIPAA? HIPAA establishes national privacy and security standards to secure an individual's protected health information (PHI),[16] as described:

- ***The Privacy Rule*** governs the use and disclosure of all forms of PHI, setting boundaries and requiring patient consent for most uses. It also grants patients rights over their own health information, including access and the ability to request corrections.

- ***The Security Rule*** focuses specifically on electronic PHI (ePHI), mandating administrative, physical, and technical safeguards to ensure confidentiality, integrity, and availability of an individual's ePHI.

APPENDIX 2

Federal Privacy and Security Laws Impacting Public Health Information Technology and Interoperability

As part of assessing and adopting new public health information technologies, a review of relevant laws is important. Some interoperability approaches involve sharing data with the federal government. This is a working list of federal laws that may impact data sharing with the federal government:

- **The Privacy Act** (5 U.S.C. § 552a) generally addresses when and to whom federal agencies may release individually identifiable information held within certain types of defined systems.[17] It also requires agencies to publish System of Records Notices describing "the types of information contained in the records, the legal authority for collecting and maintaining the records," and how the records may be used.[18]

- **Health Insurance Portability and Accountability Act Privacy Rule** (45 CFR Part 160 and Part 164). HHS issued "The Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") to implement the requirements of HIPAA to create "a set of national standards for the protection of certain health information."[19]

- **Assurances of Confidentiality-Public Health Services Act** (42 U.S.C. § 242m(d)) can be issued to protect identifiable information of individuals and institutions.[20]

- **Certificates of Confidentiality—Public Health Services Act** (42 U.S.C. § 241(d)). If research is conducted by a federal agency or is supported by federal funding, the Department of Health and Human Services is required to issue a Certificate of Confidentiality protecting the research data.[21]

- **Confidential Information Protection and Statistical Efficiency Act** (44 U.S.C. §§ 3561 et seq.). "Protects identifiable information collected by federal [statistical agencies or units] exclusively for statistical purposes."[22]

- **E-Government Act of 2002** (44 U.S.C. § 3601 et seq.). Before an agency "develop[s] or procure[s] new information technology" or changes existing technology that deals with identifiable data, it must conduct a Privacy Impact Assessment to determine how identifiable data will be "collected, stored, protected, shared, and managed" to ensure privacy protections have been incorporated "throughout the entire life cycle of a system."[23]

- **Federal Information Security Modernization Act of 2014** (44 U.S.C. §§ 3551 et seq.). Information security policies for federal agencies are generally set by the Department of Homeland Security and information security practices are overseen by the Office of Management and Budget.[24] This statute also requires the HHS Office of Inspector General to conduct an annual audit of the agency's security programs and practices.[25]

- **Federal Records Act** (44 U.S.C. §§ 2101 et seq., 2901 et seq., 3101 et seq. & 3301 et seq.). Provides foundational requirements for the management of information by federal agencies. Under the Federal Records Act, agencies must adopt "records schedules," sometimes called record control schedules, that set timelines for when records are transferred to storage, when records may be destroyed, and when records may be transferred to the National Archives and Records Administration for historical preservation.[26]

- **Freedom of Information Act** (5 U.S.C. § 552) allows the public to request access to information from federal agencies.[27] The statute applies broadly to almost any information that is maintained by an agency.[28]

- **Data Interchange Standards**. The CDC Public Health Information Network provides a list of laws and regulations that impact data interchange standards.

Citations

[1] CDC. "Data Integration Building Blocks." https://cdcgov.github.io/dibbs-site/. Accessed 6-16-2025.
[2] CDC. "About National Electronic Disease Surveillance System Base System (NBS)." February 21, 2024. https://www.cdc.gov/nbs/php/about/index.html. Accessed 6-16-2025.
[3] ASTP. "TEFCA." https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca. Accessed 6-16-2025.
[4] Bsharah, S, Sandoval, V. "Data Modernization Primer: Guide for State and Territorial Health Officials." ASTHO. May 2025. https://www.astho.org/49c2d1/globalassets/report/dm-primer.pdf. Accessed 6-16-2025.
[5] Hall K, Mwaungulu G, Pagan D. "Lawyer Up to Level Up: Engaging Legal Counsel to Bolster Public Health." July 13, 2022. https://www.naccho.org/blog/articles/lawyer-up-to-level-up-engaging-legal-counsel-to-bolster-public-health. Accessed 5-13-2025.
[6] NPHL. "Pathways to Yes: A legal Framework for Achieving Data Sharing for Health, Well-Being, and Equity." October 18, 2022. https://www.networkforphl.org/resources/pathways-to-yes-a-legal-framework-for-achieving-data-sharing-for-health-well-being-and-equity/. Accessed 5-13-2025.
[7] ASTHO. "Profile of State and Territorial Public Health." 2022. https://astho.shinyapps.io/profile/. Accessed 6-16-2025.
[8] ASTHO. "Data Modernization Tactical Guide: Identifying and Implementing Data Modernization Projects." May 2025. https://www.astho.org/49c131/globalassets/report/dm-identifying-implementing-projects.pdf. Accessed 6-18-2025.
[9] NPHL. "Conference Session: Data Governance Models." October 2019. Accessed June 17, 2025. https://www.networkforphl.org/wp-content/uploads/2020/07/Steve-Gravely-Data-Governance-Session.pdf
[10] NPHL. "Pathways to Yes: A legal Framework for Achieving Data Sharing for Health, Well-Being, and Equity." October 18, 2022. https://www.networkforphl.org/resources/pathways-to-yes-a-legal-framework-for-achieving-data-sharing-for-health-well-being-and-equity/. Accessed 5-13-2025.
[11] Hawn Nelson, A., Kemp, D. June 2022. "Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration. Actionable Intelligence for Social Policy." https://aisp.upenn.edu/resource-article/finding-a-way-forward-how-to-create-a-strong-legal-framework-for-data-integration/. Accessed 7-6-2025.
[12] FedRAMP. "FedRAMP." https://www.fedramp.gov/. Accessed 6-17-2025.
[13] GovRAMP. "About Us." https://govramp.org/about-us/. Accessed 6-17-2025.
[14] HHS. "Covered Entities and Business Associates." August 21, 2024. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html. Accessed 6-13-2025.
[15] NPHL. "Becoming a hybrid entity: As defined by the HIPAA privacy.." https://www.networkforphl.org/wp-content/uploads/2020/01/Becoming-a-Hybrid-Entity-As-Defined-by-the-HIPAA-Privacy-Rule-4-23.pdf. Accessed 6-17-2025.
[16] ASTP. "Health IT Playbook." March 11, 2020. https://www.healthit.gov/playbook/privacy-and-security/. Accessed 6-16-2025.
[17] 5 U.S.C. § 552a. Note that the Privacy Act also provides individuals with a right to access their personal information, and to request corrections and an accounting of disclosures, comparable to similar provisions under HIPAA; see 5 U.S.C. §§ 552a(a)(4), (a)(6) & (b) (defining "record," "system of record," and regulating release of records held within a system of record).
[18] HHS. "HHS system of records notices (SORNs)." April 11, 2023. hhs.gov/foia/privacy/sorns/index.html; see also, 5 U.S.C. § 552a(e)(4). Accessed 5-13-2025.
[19] HHS. "Summary of the HIPAA Privacy Rule." Updated March 14, 2025. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html; 42 U.S.C. 1320d et seq. Accessed 5-11-2025.
[20] CDC. "Protecting Privacy and Confidentiality." Updated February 13, 2025. https://www.cdc.gov/scientific-integrity/php/protecting-privacy-confidentiality/. Accessed 5-12-2025.
[21] 42 U.S.C. § 241(d).
[22] NPHL. "Confidential Information Protection and Statistical Efficiency Act of 2002 Snap Shot." 2018. networkforphl.org/wp-content/uploads/2020/01/Snapshot-CIPSEA.pdf. Accessed 5-12-2025.

[23] National Archives and Records Administration. "E-Government Act of 2002." https://www.archives.gov/about/laws/egov-act-section-207.html. Accessed 5-9-2025.
[24] Cybersecurity & Infrastructure Security Agency (CISA). "Federal Information Security Modernization Act." cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act. Accessed 5-9-2025.
[25] HHS-Office of Inspector General. "About OIG." https://oig.hhs.gov/about-oig/. Accessed 5-12-2025.
[26] HHS. HHS Policy for Records Management. Note 3 at 6.1.2.1 NARA-Approved Records Retention Schedules.
[27] US Department of Justice. Office of Information Policy. "What is the FOIA?" foia.gov/faq.html. Accessed 5-12-2025.
[28] 5 U.S. Code § 552(f)(2)).