Washington State Public Health Data Sharing Law & Policy Review

Final Report

(As of May 31, 2024)

James G. Hodge, Jr., J.D., LL.M.
Peter Kiewit Foundation Professor of Law
Director, Center for Public Health Law & Policy
ASU Sandra Day O'Connor College of Law
james.hodge.1@asu.edu

Jennifer L. Piatt, J.D.
Research Scholar
Co-director, Center for Public Health Law & Policy
ASU Sandra Day O'Connor College of Law
Jennifer.Piatt@asu.edu

Erica N. White, J.D.
Research Scholar
Center for Public Health Law & Policy
ASU Sandra Day O'Connor College of Law
ericawhite@asu.edu

Citation: Hodge, Jr. JG, Piatt JL, White EN. Washington State Public Health Data Sharing Law & Policy Review: Final Report. Washington State Department of Health, Olympia, WA: 2024: 1-56.

PREFACE

Acknowledgements. This report was developed by **James G. Hodge, Jr.**, **J.D., LL.M.**, Peter Kiewit Foundation Professor of Law and Director; **Jennifer L. Piatt, J.D.**, Research Scholar and Co-Director; and **Erica N. White, J.D.**, Research Scholar, at the Center for Public Health Law & Policy (CPHLP), Sandra Day O'Connor College of Law, Arizona State University (ASU). Additional contributions were made by **Mary Saxon, J.D., Heather McCoy, J.D.**, **Isabella Goldsmith, J.D., Camille Laude**, and **Kyrah Berthiaume**, CPHLP Legal Researchers. Many thanks to **Leila F. Barraza, J.D., M.P.H.**, Associate Professor, Zuckerman College of Public Health, University of Arizona, and **Cason Schmitt, J.D.**, Assistant Professor, Texas A&M University School of Public Health, for their expert reviews and comments on an initial working draft of the report. **Francoise Pickart. M.P.H.**, WA DOH Data Democratization lead, and numerous other colleagues from Washington State provided expert review and comments on a complete draft of the report.

Funding. Funding for this project was provided by the Washington State Department of Health via interagency agreement with ASU from 9/15/23 – 7/31/24.

Disclaimer. Information provided in this document does not constitute legal advice in Washington State or any other jurisdiction. Please consult with the Washington State Office of the Attorney General, or legal counsel in your respective jurisdiction, for specific legal advice.

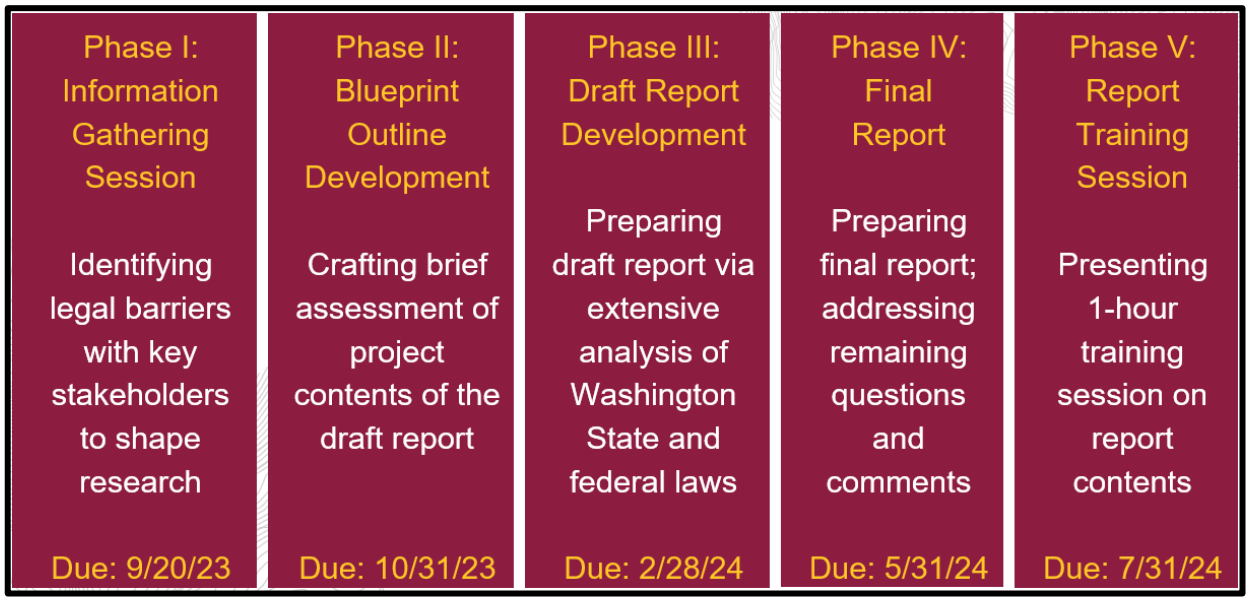
Scope*.* Access to accurate and reliable health data is key to effective and ethical public health practices. However, legal and policy requirements can present perceived or actual barriers to data sharing or exchanges. Numerous statutes, regulations, judicial interpretations, and policies at state and federal levels shape the acquisition, use, disclosure, and exchange of public health data. Laws and policies authorize public health data collection for surveillance, reporting, or research purposes, but may also limit these activities in the interests of privacy, anti-discrimination, and security. Balancing these dynamic facets—authorizing data exchanges, protecting privacy, avoiding discrimination, and assuring security—is essential to achieving improved population health outcomes through legally- and ethically-sound data sharing practices.

As per the **Project Timeline** below, this project examines the law and policy framework underlying public health data sharing in Washington State based on an assessment of relevant federal and state statutes, regulations, case law, and applicable agency policy interpretations through February 28, 2024. This report evaluating the legal landscape surrounding public health data sharing in Washington State identifies strengths, weaknesses, and opportunities for improvements. The goal is to enable public health agents and their partners to legally navigate public health data sharing practices in Washington State in promotion of communal health.

Limitations. Though comprehensive, this project does not attempt to exhaustively assess or list all Washington State laws and policies impacting public health data sharing and does not include extensive tables of all statutes or regulations directly or tangentially

impacting public health data sharing. The focus on state-level laws precludes closer reviews of local laws and legal distinctions. This project also does not assess or provide guidance on technological or IT-based topics contributing to data sharing issues. Finally, this report reflects the outside legal and policy perspectives of public health law researchers at the Sandra Day O'Connor College of Law, ASU, guided by internal resources and reviews among WA DOH and other Washington State public health data leaders, practitioners, and reviewers.

Project Timeline



ABBREVIATIONS

Please note that these acronyms, listed alphabetically, are used throughout the report without further definition in the body of the report.

Acronym	Term	Acronym	Term
ADA	Americans with Disabilities Act	**NAM**	National Academy of Medicine
AGO	Attorney General Opinion	**NCHS**	National Center for Health Statistics
AI	Artificial Intelligence	**NGO**	Non-Governmental Organization
AI/AN	American Indian/Alaska Native	**NIST**	National Institute of Standards & Technology
BRFSS	Behavioral Risk Factor Surveillance System	**NSSP**	National Syndromic Surveillance Program
CDC	Centers for Disease Control & Prevention	**OCR**	Office of Civil Rights (HHS)
CHARS	Comprehensive Hospital Abstract Reporting System	**OCS**	Office of Cybersecurity (WA State)
CHAT	Community Health Assessment Tool	**PHA**	Public Health Agency/Authority

Acronym	Term	Acronym	Term
CMS	Centers for Medicare & Medicaid Services	**PHE**	Public Health Emergency
CSC	Crisis Standards of Care	**PHI**	Protected Health Information
DSA	Data Sharing Agreement	**PHIMS**	Public Health Issue Management System
DUA	Data Use Agreement	**PMP**	Prescription Monitoring Program
eHARS	enhanced HIV/AIDS Reporting System	**PRA**	Public Records Act (WA State)
EMS	Emergency Medical Services	**RCW**	Revised Code of Washington
EMT	Emergency Medical Technician	**RHINO**	Rapid Health Information Network
FDA	Food & Drug Administration	**SHELDIn**	Sexually Transmitted Disease Hub for Electronic Laboratory Data Input
FERPA	Family Educational Rights & Privacy Act	**SME**	Subject Matter Expert
GCD	General Communicable Diseases	**STI**	Sexually Transmitted Infection
HCP	Health Care Provider	**SUD**	Substance Use Disorder
HHS	Department of Health & Human Services	**TB**	Tuberculosis
HIPAA	Health Insurance Portability & Accountability Act	**UHCIA**	Uniform Health Care Information Act
HIV	Human Immunodeficiency Virus	**WAC**	Washington Administrative Code
HSR	Human Subjects Research	**WA DOH**	Washington State Department of Health
IHI	Identifiable Health Information	**WDOC**	Washington Department of Corrections
IHS	Indian Health Service	**WaTech**	Washington Technology Solutions
IRB	Institutional Review Board	**WDCYF**	Washington Department of Children, Youth & Families
LHJ	Local Health Jurisdiction	**WDRS**	Washington Disease Reporting System
LTCF	Long - Term Care Facility	**WDSHS**	Washington Department of Social & Health Services
MAA	Mutual Aid Agreement	**WELRS**	Washington Electronic Laboratory Reporting System
MAC	Multi-Agency Cooperation	**WEMSIS**	Washington Emergency Medical Services Information System
MHCC	Medical & Health Coordination Center	**WSHCA**	Washington State Health Care Authority
MHMDA	My Health My Data Act (WA State)	**WSIRB**	Washington State Institutional Review Board
MSPHPA	Model State Public Health Privacy Act		

TABLE OF CONTENTS

INTRODUCTION/EXECUTIVE SUMMARY

Protecting the public's health requires ready access to accurate, timely, and reliable health information derived from patient data, resident surveys, and other sources. Identifiable health data are the life blood of public health practice and research. Assuring interjurisdictional access to meaningful IHI across multiple types and sources of data, however, presents substantial challenges for PHAs. At play in modern public health data exchanges are profound risks to privacy, potential discrimination, and security breaches.

States like Washington have attempted over the years to address these risks while assuring ready access to essential health data through manifold state laws, policies, and procedures governing data acquisition, use, and exchange. Interwoven with federal data sharing laws and requirements, Washington State public health laws and policies greatly shape data exchanges between and within state, tribal, and local PHAs, HCPs, and others. A laudable goal underlying these laws and policies is to promote the public's health through effective data sharing and management while preserving individual and group-related privacy, anti-discrimination, and other protections. Yet, complying with multifarious, layered information laws and policies over time can lead to (1) confusion for those sharing and accessing data, (2) delays or denials of essential public health data sharing, or (3) cessation of public health interventions relying on data flows.

Balancing needs to exchange health data, protect privacy, avoid unwarranted discrimination, and assure data security is imperative to achieving improved population health outcomes through lawful and ethical data exchanges. Given substantial public health data sharing challenges regularly experienced among public and private sectors in Washington State, this Report assesses relevant laws and policies, examines opportunities for improved data sharing, and proposes potential legal options for further consideration among law- and policy-makers.

I: PUBLIC HEALTH DATA ACQUISITIONS & USES examines select laws and policies in Washington State authorizing public health data collection for surveillance, reporting, or research purposes. As in other states, Washington statutes and regulations expressly allow for widespread data acquisitions and exchanges for disease- and condition-specific surveillance. Public health reporting laws require HCPs and others to share IHI with state and local PHAs, and enable interjurisdictional data sharing of acquired information, typically without individual informed consent or authorization. Thus, state PHAs can share data with localities, and vice versa. As per federal- and state-level requirements, IHI shared for public health practice must be distinguished from public health research activities pursuant to differing legal and ethical exchange standards.

Protecting health information privacy is a major focus of Washington State laws and policies, as examined in **II: PUBLIC HEALTH PRIVACY, ANTI-DISCRIMINATION & SECURITY**. Conscientious of the profound risks to personal privacy and concomitant potential for discrimination, Washington has enacted or promulgated numerous privacy provisions coupled with anti-discrimination protections for specific persons or populations. Some of these privacy laws and policies may mimic federal requirements like the HIPAA

Privacy Rule, although the Rule does not apply to most public health data exchanges. Other Washington State privacy laws supplement federal protections, contributing to interpretive dilemmas in enforcement and conflicts in data exchanges under differing standards.

Privacy and anti-discrimination challenges are compounded by public concerns and general mistrust, especially following the COVID-19 pandemic (2020–2023) when federal and state emergency laws allowed for extensive modifications of data privacy practices. Efforts to assure the security of identifiable data have led to a bevy of additional laws and practices in the State necessitating data stewardship approaches and execution of various agreements that have collectively derailed some data exchanges despite clear public health objectives underlying their acquisition and use.

Some laws and internal policies in Washington State reflect protectionary approaches that may obfuscate data flows and exchanges. Resulting levels of confusion and unpredictability of routine or emergency data practices are undergirded by varying data-specific requirements tied to conditions, populations, or entities. As examined in **III: NAVIGATING PUBLIC HEALTH DATA SHARING PRACTICES**, charting a course through these diverse practices in Washington State can be difficult. State and local PHAs rely heavily on legal requirements and corresponding agency policies to execute DSAs to facilitate the flow of IHI between federal-state-tribal-local agencies.

While public health data sharing practices in Washington State may present robust protections, opportunities exist to improve or hasten information exchanges without compromising privacy, implicating discrimination, or threatening security. An array of options to promote data sharing practices across the State is proposed in **IV: PATHWAYS TO IMPROVED PUBLIC HEALTH DATA SHARING**. A series of scoping themes underlying affirmative public health data practices are set forth and illustrated as related to Washington State laws and practices. Among the preeminent goals is authorizing real-time public health data exchanges between state, tribal, and local PHAs without unnecessary "red tape" requirements and resulting delays.

As in other states, consideration of model public health data sharing principles may result in freer flows of IHI in promotion of health equity without compromising individual or group privacy. Ultimately, the Report offers a series of legislative or regulatory reforms in Table 1 for policymakers considering ways to remedy difficult legal conflicts or entrenched policies. These prospective legal and policy recommendations gleaned both from this assessment and from input from practitioners and policy-makers in Washington State may promote efficient data sharing practices for the future, subject to the discretion of state and local lawmakers and their constituents.

I: PUBLIC HEALTH DATA ACQUISITIONS & USES

As the leading PHA in Washington State, WA DOH operates pursuant to a broad statutory mission to "improve illness[,] injury prevention[,] and health promotion" and ensure "quality health services."[1] To this end, the Department coordinates with the Washington State Board of Health, as well as local and tribal PHAs,[2] in acquiring, using, and sharing health data that are "integral" to core public health services.[3] Such data include information aiding PHAs in "inspecting and improving the public's health through prevention and control of infectious and noninfectious conditions."[4]

Responsible data sharing practices in Washington State entail affirmative laws and policies balancing the inflow of IHI from numerous sources to state and local PHAs entrusted with their privacy, security, and safe handling (see **II**). Washington State and local PHAs are legally authorized to acquire IHI and other data for public health surveillance, investigations, research, and other activities. Described below, these laws authorize PHAs to collect and appropriately use these data for public health purposes, often without individual informed consent.

A. PUBLIC HEALTH SURVEILLANCE & REPORTING

Public health surveillance entails the "ongoing systematic collection, analysis, and interpretation of data" by PHAs to assure population-level awareness of disease, injury, and other conditions.[5] Surveillance and epidemiologic investigations are essential to detect, prevent, and control public health threats through acquisition and analyses of real-time information on population health status, behaviors, and outcomes. Manifold federal, state, and local laws undergird public health data collections and uses. While federal PHAs like CDC routinely receive public health surveillance data through varied legal authorities, this information is typically collected initially at the state and local levels. State-level public health surveillance laws may set distinctions based on the original purpose of the collected data, determining when and how data may be shared. These distinctions are critical to ensuring timely notice to public health decision-makers to facilitate well-informed resource allocations and policy decisions.

1. Authorized Surveillance Activities

Each state maintains public health surveillance systems to monitor (1) reportable infectious disease conditions; (2) noninfectious conditions; and (3) other public health indicators.[6] These systems are typically populated via data acquired through State legal reporting requirements prescribing regular sharing of IHI or other health data to state or local PHAs. The Washington State legislature has created several public health reporting systems. As summarized below, WDRS[7] is typically used for "notifiable conditions," RHINO[8] for emergency department data, SHELDIn for STIs, eHARS for HIV/AIDS, CHARS[9] for hospital stay data, and CHAT for population-level risk behaviors.[10]

WDRS is a comprehensive electronic surveillance system through which WA DOH receives, manages, and analyzes public health data and related information from local

community reporters (e.g., clinics, labs, hospitals, local HCPs, and "other non-health care sources").[11] WDRS supports 4 disease groups: (1) general communicable diseases (GCDs); (2) Hepatitis (except A and E, which are part of GCD); (3) blood lead; and (4) TB.[12] Reports from HCPs are shared with WDRS or local LHJs without express, specific informed consent of patients or others.[13] The system is designed to facilitate secure communication and coordination between WA DOH and locales to ensure effective, timely public health interventions (e.g., investigations, monitoring, contact tracing) while respecting individual privacy via use of non-identifiable data (see **II.A**).[14]

RHINO entails extensive "syndromic surveillance data collection, analysis, and distribution" which WA DOH uses to identify and investigate emerging public health threats.[15] Emergency departments across the state are statutorily required to submit electronic syndromic surveillance data to RHINO.[16] These intake data, which include patient demographic information, chief complaint, and diagnosis codes, may also be collected in "near real-time" from eligible onboarded registrants including hospitals, clinics,[17] primary care providers, and select specialists (e.g., behavioral health professionals).[18] Statutes regarding health risk behavior and violence data specifically allow WA DOH to contract with higher education institutions experienced in data collection "relating to the health and overall welfare of children" for additional public health research purposes.[19] While non-emergency HCPs are not required to participate in RHINO, they may voluntarily pre-register to provide related data.[20] RHINO data may be available on request to public or private requestors in "original or processed form," within a certain time period, if additional conditions are satisfied.[21]

STI (including HIV/AIDS) data are collected via electronic laboratory and case reporting systems and disease investigation services. SHELDIn is used to deliver STI laboratory reports as well as store standardized laboratory reports from multiple sources to facilitate statewide data access and public health services.[22] Statewide HIV/AIDS data are collected in eHARS.[23]

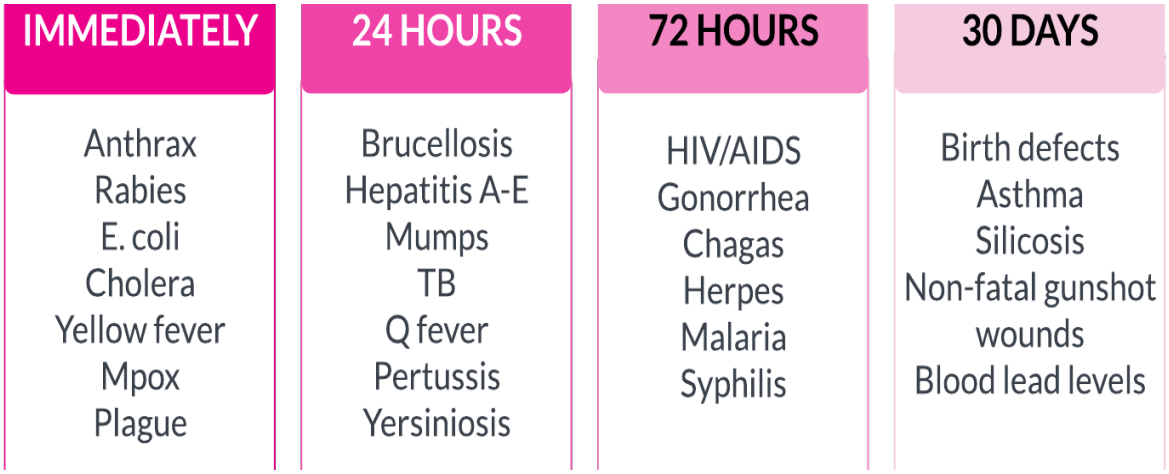
CHARS collects inpatient and observation data from patient stays at community hospitals to identify and analyze state-wide hospitalization trends.[24] WA DOH is statutorily required to develop rules for the acquisition and use of violence, at-risk behaviors, and other risk-related data.[25] As sole coordinator, WA DOH must provide data to LHJs and other local stakeholders to use in community program planning and evaluation.[26] In 2021, the Washington State legislature amended existing laws to require hospitals reporting patient discharge data through CHARS to include information on race, ethnicity, gender identity, sexual orientation, preferred language, disability, and zip code.[27]

WA DOH reviews specific risk-related health data to input into another system, CHAT, its secure online system for population data storage, which is also used by other state, tribal, or local PHAs.[28] CHAT includes data on pregnancy, fertility, abortion, birth risk factors, communicable diseases, cancer incidence, hospitalizations (including injuries), deaths, and other risk-related information. An additional pre-hospital tool, WEMSIS, is used for emergency medical data.[29]

2. Specific Reporting Requirements

Suspected or known cases of conditions subject to public health surveillance are required to be reported by HCPs and facilities, laboratories, and veterinarians, among others, through standardized data systems for notifiable conditions, including WELRS,[30] WDRS,[31] and SHELDIn.[32] State laws and policies dictate the timing, content, and scope of reportable information. As illustrated in **Figure 1**, below, select highly infectious conditions are "immediately" reportable, while data concerning other serious infectious conditions (or those requiring lab pathology results) must be shared within 24 hours to 3 business days. Certain non-communicable or chronic conditions are reportable within 30 days. Most of these conditions are typically reported first to LHJs. HIV infections and CD4 counts (immune cell indicators used to assess HIV/AIDS), however, are reported directly to WA DOH.

Figure 1. Washington State Select Reportable Conditions



Additional administrative regulations require HCPs and facilities to provide specified information on each case report, including the patient's first and last name; address; date of birth; sex; ethnicity; race; preferred language; contact phone number; diagnosis or suspected diagnosis; and laboratory results if available.[33] Required information also includes the principal HCP and contact number; address where care was received; and name and contact phone number of the person providing the case report.[34] For select conditions, such as Hepatitis B, a patient's pregnancy status is reportable, subject to specific protections for reproductive health information (see **III.A.1**). WA DOH and LHJs may request additional information from HCPs[35] and labs.[36]

As a primary holder of public health surveillance data, WA DOH is required to:

a. develop "routine data dissemination mechanisms" that describe and analyze notifiable conditions case investigations and data;[37]
b. distribute "periodic" epidemiological reports;

c. conduct an annual review of "public health issues" for state PHAs and officers;[38]
d. make case investigation documentation for notifiable conditions available to LHJs and others within 24 hours of receipt; and
e. share "other data" for use in case investigations and other epidemiological reports available to PHAs within 2 business days of request.[39]

3. Local-Level Distinctions in Surveillance Activities

HCPs and facilities are legally obligated to involve state PHAs as well as authorities in the 35 LHJs across the State (see **Figure 2**) concerning known or suspected reportable conditions. HCP case reports must be shared with WA DOH or appropriate LHJs based on requirements for specific notifiable conditions set out in Washington statutes and regulations (see **III.A**). HCPs are generally required to notify LHJs of the patient's residence (if known).[40] Immediately notifiable conditions including anthrax, measles, and smallpox necessitate real-time teleconference reporting to LHJ 24/7 hotlines as soon as clinically suspected. Conditions notifiable within 24 hours, such as Hepatitis A-E, should be reported via phone during normal public health business hours. Conditions reportable within 3 business days are typically made by the facility instead of the diagnosing HCP.

Figure 2. Local Health Jurisdictions[41]

Select localities may have unique reporting standards or requirements supplementing State protocols.[42] For example, King County has distinct hotline phone numbers for specific conditions including HIV/AIDS and TB.[43] Pursuant to Washington State administrative requirements and guidance, LHJ officers review and determine

appropriate actions for each case of a notifiable condition or suspected outbreak based on the threat to public health.[44] LHJs are also responsible for (a) establishing systems to maintain confidentiality; (b) notifying HCPs, labs, and facilities about requirements and pending investigations; (c) authorizing contact tracing; and (d) sharing cases of reportable conditions with WA DOH.[45]

As the State's designated central public health data resource, WA DOH legally must:[46]

a. provide, upon request, technical assistance to LHJs, other state agencies, HCPs, facilities, and labs investigating notifiable conditions;
b. maintain a 24/7 hotline for reports of immediately-notifiable conditions;
c. consult with requesting HCPs, facilities, and labs obliged to comply with reporting requirements; and
d. "negotiate alternatives" for reporting requirements through cooperative agreements between HCPs, facilities, labs, and agencies that provide the same level of public health protection as statutory reporting mechanisms.[47]

WA DOH is not limited to receiving specified information about notifiable conditions. It is authorized to receive health care and other data beyond what is statutorily required.[48] LHJs also may be entitled to receive specific information. In 2024, for example, the Washington legislature considered a bill to allow LHJs to retain IHI and geographic information relating to child fatalities for trend analysis.[49]

4. Public Health Service Delivery & Activities

Washington's legislature statutorily defined the State public health system as including "foundational public health services" and a "public health services improvement plan" in 2019.[50] This plan includes minimum standards for public health assessment and policy development, with data collection and reporting requirements developed by WA DOH.[51] Several state laws require WA DOH to establish specific public health programs (e.g., domestic violence education,[52] supplementary HIV insurance coverage,[53] opioid response[54]), but do not specifically require distinct data use policies. In 2020, the legislature required WA DOH to generate information for HCPs regarding requirements and authority for medical information dissemination,[55] largely deferring to WA DOH to develop public health data sharing policies.

B. PUBLIC HEALTH RESEARCH

In addition to routine uses of IHI for public health surveillance, evaluation, or other core public health activities, PHAs may also seek and use IHI for public health research. The ability of PHAs to conduct ethical research in Washington State is unquestioned: research, like other interventions, is essential to assuring the public's health. Legal and ethical dilemmas typically arise, however, in determining exactly what constitutes public health "research" versus public health "surveillance" or other related "activities." These distinctions are key since acquisition and use of IHI for research purposes entail different

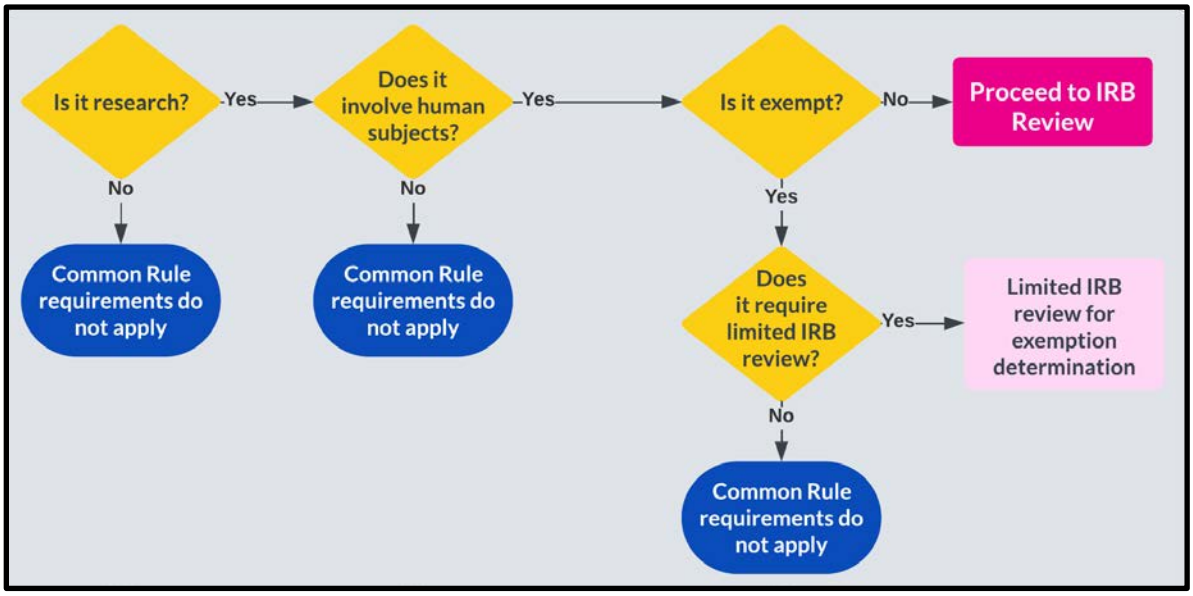
legal routes, ethical norms, or specific requirements designed to limit unauthorized disclosures and prevent unintended risks of harm to research subjects.

1. Permissible Acquisitions & Uses

Like surveillance, public health research can enhance interventions and offer new approaches to addressing communal health challenges. Conducting research on identifiable human subjects or their IHI, however, requires safeguards to avoid abuses, breaches, or other harms.[56] The federal Common Rule[57] establishes core protections applicable to manifold federal agencies and their funded research projects.[58] HSR is defined via the Common Rule as "a systematic investigation . . . designed to develop or contribute to generalizable knowledge."[59] Multiple states, including Washington, largely adhere to the Common Rule in their jurisdictions,[60] subject to other state, tribal, and local laws and policies providing additional protections. WSIRB is responsible for review, approval, and oversight of HSR in Washington State.

As per **Figure 3**, the Common Rule requires informed consent and IRB review, among other provisions, of covered, non-exempt research.[61]

Figure 3. Common Rule Applications[62]



Common Rule provisions do not apply to "exempt" research (1) that does not acquire or use IHI; or (2) whose data would not harm subjects if disclosed (often because it is non-identifiable).[63] What constitutes IHI for HSR purposes is fungible. IHI includes any information from HCPs concerning an individual's medical conditions, receipt of health care services, or the payment of such services that may be used to identify the individual.[64]

Departments and agencies must regularly re-examine what comprise "identifiable private information" and "identifiable biospecimens" based on modern technologies.[65] At the federal level, HHS regularly revisits these definitions under the Common Rule. WDSHS lists several research categories exempt from review through its human research review board or a departmental service unit research oversight committee.[66]

Washington State requirements governing HSR data acquisitions and uses largely parallel federal requirements, with some exceptions. The State has crafted its own definition of "research" for purposes of records release which ties to academic, research professional, or agency pursuit of scientific knowledge, evaluation, or problem solving on several specific topics.[67] Distinctions in interpretation and application of the definition of research among governmental officials can complicate and slow progress towards providing timely public health action and accomplishing research goals.[68]

Pursuant to the Common Rule, IRBs must ensure "adequate provisions . . . to maintain the confidentiality of data," which manifest in research confidentiality agreements.[69] Washington State law and policies require research organizations to execute detailed confidentiality agreements with state agencies providing IHI[70] and prohibit participation in HSR unless approved by WSIRB.[71] Research proposals requiring expertise beyond that held by the HSR review board's members necessitate further consultation with at least 4 research experts as to the proposal's merit, benefits, and risks.[72] Washington State agencies can seek reimbursement of research assistance costs, including screening records for sampling, extracting information, and performing statistical analysis.[73]

2. Consent & Disclosure Requirements

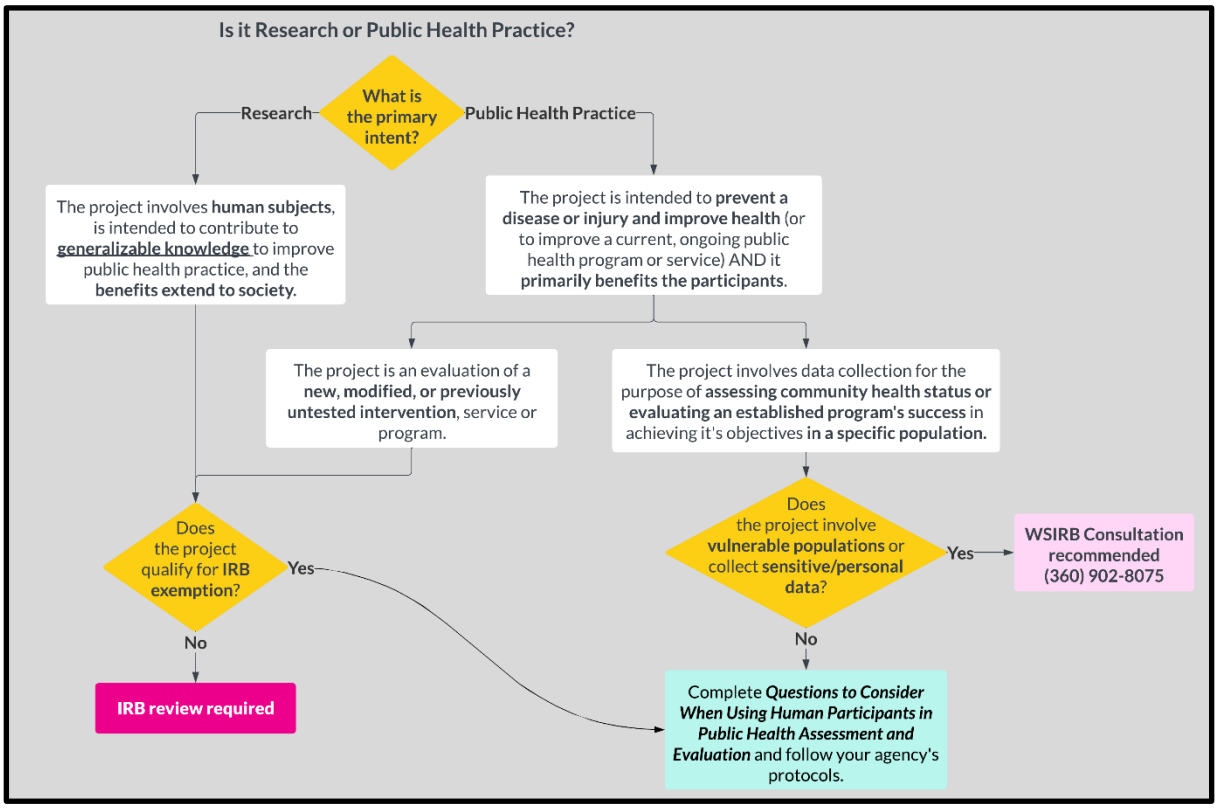
Research consent and disclosure requirements are intended to protect research subjects' rights and welfare.[74] Under the Common Rule, consent forms must provide information a reasonable person would seek, including research purpose(s), research study duration, and select risks or benefits.[75] What is known as "broad consent" under the Common Rule can be used for storage, maintenance, and secondary research uses of private data or biospecimens with fewer required elements.[76]

Washington State agencies can provide access to or copies of IHI records for research with participants' written informed consent.[77] Access may also be provided without consent if: (a) agencies have specified rules relating to "research review and approval;" (b) disclosures are consistent with federal law; and (c) agencies negotiate confidentiality agreements with researchers prior to any disclosures.[78] To avoid potential HSR infringements and resulting penalties,[79] PHAs can informally consult with IRBs to ascertain if a proposed HSR project requires full IRB review based on the sensitivity of subjects or data involved.[80] Researchers may only disclose IHI in limited situations including those related to a risk of injury to a person or pursuant to audits, search warrants, or court orders.[81]

3. Distinctions Between Public Health Practice & Research

PHAs must distinguish between using IHI for public health "practice" or "research" purposes to comply with differing legal and ethical standards underlying each activity.[82] This is not always easy. Conflicts among PHAs and IRBs attempting to draw distinctions between data sharing in these different realms can stymie public health activities.[83] Multiple sources provide decision trees, checklists, or workflow diagrams to assist practitioners in making these determinations.[84] As per the diagram exhibited in **Figure 4**, below, WA DOH and other agencies distinguish public health practice and research activities based largely on researchers' primary intent.

Figure 4. WA DOH HSR or Public Health Practice Decisions[85]



Notwithstanding such guidance, PHAs in Washington and other states may still disagree over what constitutes "research" or "practice," as illustrated in **Focus 1** below.

Focus 1 – Use of PMP Data for Research

Like most states, the Washington State PMP tracks prescription drug dispensing records for select medications with a high risk for abuse, such as opioids. Washington State regulations and statutes identify these data as confidential and thus non-accessible. Still, state law provides limited exemptions from these confidentiality requirements for physicians and pharmacists; licensing, certification, or state regulatory agencies; and others. WA DOH may also allow public and private entities to access these data for "statistical, research, or educational purposes" without IRB authorization. Several distinct statutory pathways for data use can obfuscate whether and to what extent additional procedures are required (e.g., IRB review, DSA execution), hindering data exchanges for such purposes as provided for in State law.

In 2018, the Common Rule was revised to enhance protections for research participants and reduce unnecessary burdens on researchers by matching oversight to the research project's level of risk.[86] The revised Rule explicitly clarified that public health "surveillance" is not "research." Under federal law, surveillance activities thus do not require informed consent and IRB approval requirements like HSR.[87] Despite these clarifications, debates over the classification of public health practice and research activities continue in part to assure health information privacy and promote anti-discrimination protections, as examined more closely in **II**.

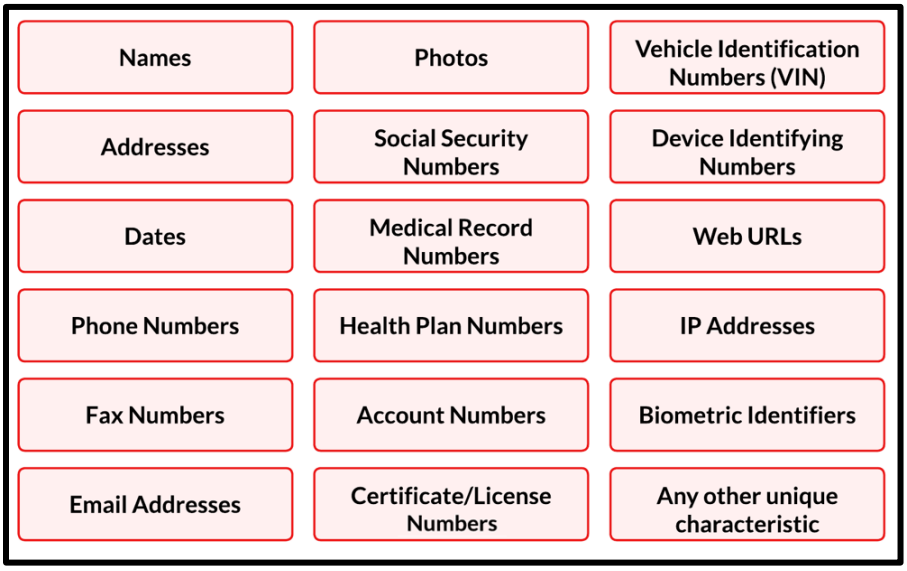
II: PUBLIC HEALTH PRIVACY, ANTI-DISCRIMINATION & SECURITY

Extensive federal[88] and Washington State[89] laws support public policy goals of maintaining and assuring health information privacy, preventing unwarranted discrimination, and assuring security of IHI in the interests of supporting and building trust in communal health services and functions. Still, as determined by the Washington Supreme Court in 1986, constitutional privacy and security interests are not absolute.[90] As noted in **I**, these interests must be balanced against legitimate uses of IHI for public health purposes, including surveillance, disease control and response, and research. ***Ultimately, balancing individual interests in the protection of sensitive health or other information with communal needs to access and use such data is synergistic with protecting the public's health.***[91]

A. PUBLIC HEALTH DATA PRIVACY

Many key legal requirements surrounding health data privacy hinge on whether the data at issue contain identifiers.[92] Generally, PHI includes health information that can be used to identify an individual.[93] De-identified data, on the other hand, cannot be used to identify the patient, which mitigates privacy risks while supporting data uses for essential public health purposes.[94] Specific Washington State and federal laws legally distinguish between identifiable and de-identified data largely as to whether there is a "reasonable basis" that a person who is the subject of the health information could be identified via specific data sources.[95] If so, the data is likely PHI; if not, the data can be considered de-identified (even if there is some remote chance that it may still be used to identify an individual through unwarranted or unlawful means).[96] The HIPAA Privacy Rule, as revised by the federal HITECH Act,[97] expressly lists identifiers that must be removed to assure medical records data are de-identified (see **Figure 5**, below).[98]

Figure 5. Specific HIPAA PHI Identifiers[99]

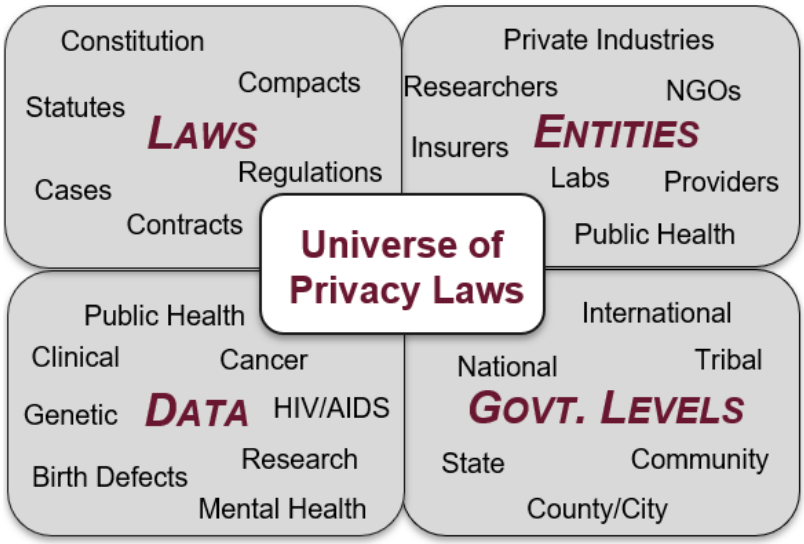


Multiple Washington State statutes address data de-identification across a variety of subject areas, including public records,[100] medical records,[101] state disability services,[102] insurance,[103] in-home services,[104] immigration,[105] and public health and safety.[106] On April 1, 2021, WA DOH issued regulations delineating identifiers in birth and fetal death records for vital statistics releases[107] and releases of patient discharge information.[108] The Department has also implemented guidance for sharing information containing "small numbers" to help eliminate the chance of positive identification of specific individuals from aggregate data.[109] Washington laws and policies do not articulate a *universal* standard as to which identifiers must be removed from data for it to be considered de-identified. Nor has WA DOH or other state agencies incorporated via reference specific approaches set forth in the HIPAA Privacy Rule as applied to IHI (see **Figure 5**).

1. Core Principles of Health Information Privacy

The legal environment surrounding health information privacy is vast. As illustrated in **Figure 6**, below, numerous health information privacy laws at all levels of government govern specific entities and particular types of data.

Figure 6. Universe of Health Information Privacy Laws[110]



Core principles of health information privacy center around ensuring that acquisitions and uses of PHI are appropriately authorized to protect the public's health while minimizing disclosures outside public health systems that may lead to discrimination and other harms. Assuring health information privacy is key to building trust with patient populations and simultaneously guarding against breaches which may result in unwarranted discrimination tied to personal health conditions. Washington State's privacy principles are illustrated below via **Figure 7**.

Figure 7. Washington State Privacy Principles[111]

As noted above, de-identification is a particularly effective means of ensuring data uses and disclosures do not trigger most state and federal privacy laws.[112] Still, certain public health activities, including surveillance and targeted interventions, necessitate sharing of IHI for accuracy and efficacy, which in turn may inform policy development. For example, sharing identifiable data related to spikes in opioid overdoses in certain locales or among specific populations can facilitate effective interventions (e.g., targeted naloxone distribution), which may later inspire policy-driven changes (e.g., placement of syringe service programs).[113] Even so, federal and state privacy laws tend to limit non-consensual disclosures of PHI to the minimum amount of data necessary to accomplish the permissible purpose for which the data are sought.[114] Under the HIPAA Privacy Rule, for example, covered entities are largely directed to defer to PHAs specific requests and justifications for IHI without questioning the PHAs' need for the data.[115]

As per **Figure 7**, additional key concepts underlying patient health information privacy include notice, consent, transparency, and accountability. Generally, as per the Privacy Rule, HCPs and facilities must inform patients of privacy practices and intended data uses.[116] Notice is not always required, however, prior to acquisition, use or disclosure of IHI for public health purposes.[117] Washington State agencies, including WA DOH, must notify individuals if their personal information is improperly disclosed.[118] Closely intertwined with notice is individual consent. Generally, consent (or authorization) is a prerequisite to sharing PHI without an applicable legal exception.[119] Transparency and accountability build trust in data handlers through respect for PHI.

Some policy justifications for disclosing PHI overwhelm the need to maintain privacy. In line with "right to know" legal requirements and ethical standards supporting greater equity in public health data systems,[120] special circumstances warrant disclosure of PHI to avert known harms to individuals or groups (e.g. "right to be counted")[121] Despite state and federal laws generally protecting the privacy of psychiatric information, the

Washington Supreme Court held in *Volk v. DeMeerleer* (2016) that such data may be subject to disclosure to ensure the safety of foreseeable victims pursuant to valid state law exceptions.[122] Coextensively, Washington statutory law authorizes HCPs, WDSHS, and WSHCA (which oversees Apple Health, the State's Medicaid program) to release information when individuals may pose dangers to others.[123]

2. Access, Use & Disclosure Requirements

At its core, protecting PHI privacy centers on legal requirements concerning permissible access, use, and disclosures of data, as well as limitations and exceptions. While the HIPAA Privacy Rule spells out required and permissible data uses and disclosures with respect to PHI, it only applies to "covered entities" including HCPs, health plans, healthcare clearinghouses, and their business associates.[124] State and local PHAs (including WA DOH) may also be considered "hybrid entities" pursuant to the Rule if they engage partially in actions which would make them a covered entity (e.g., WA DOH's newborn screening program). Other, non-covered entities, such as the vast array of PHAs collecting IHI for public health surveillance or other purposes (see **I**), do not have to adhere to the Rule directly. However, the Rule may still impact the flow of IHI to PHAs through misapplications or misinterpretations by covered entities as discussed below.

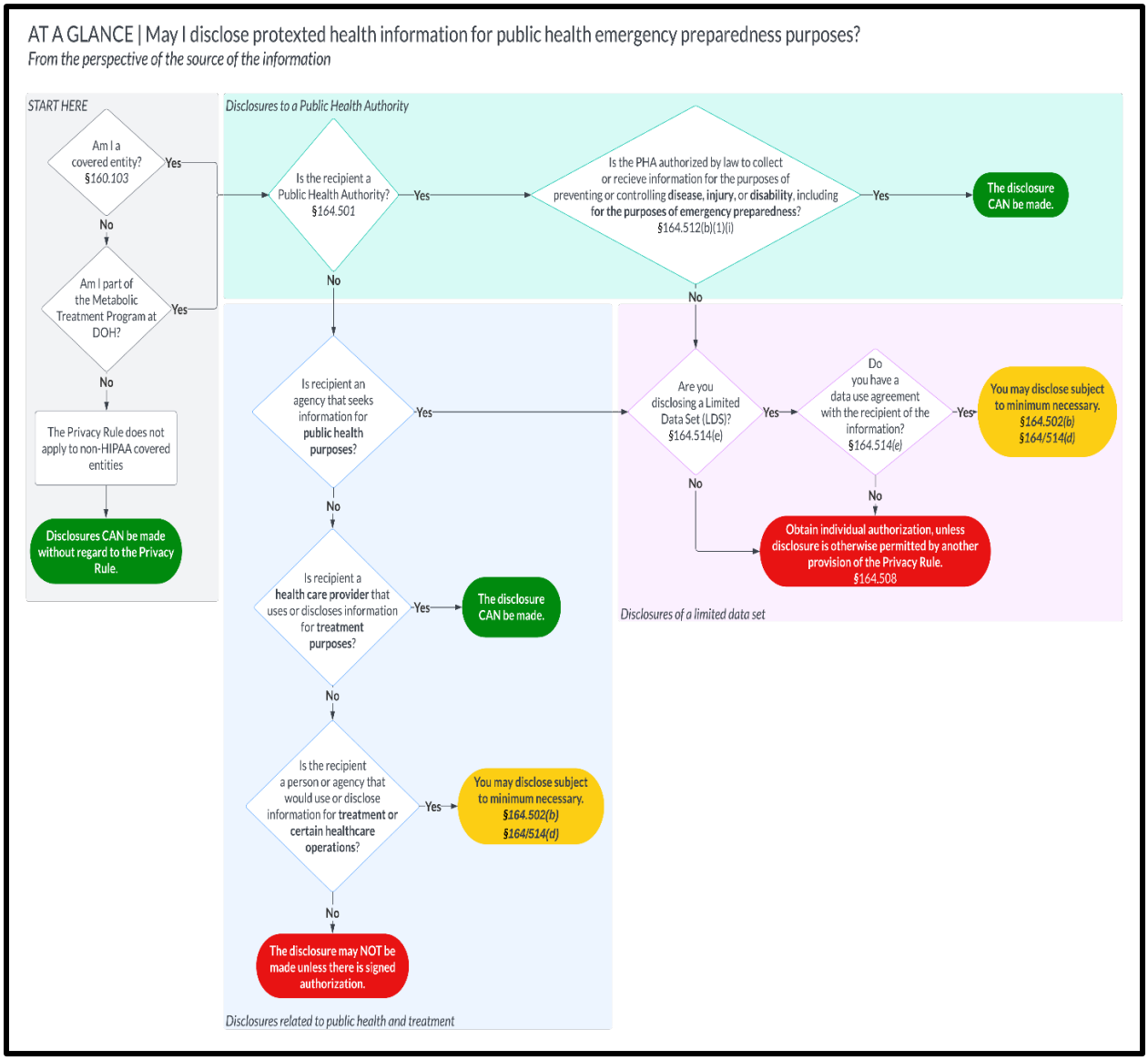
Generally, the Rule requires covered entities to seek and obtain written authorization from individuals for acquisitions, uses, or disclosures of PHI, subject to specific exceptions.[125] For example, with a valid authorization, covered entities may use PHI for limited marketing or sale purposes, or otherwise disclose PHI if not prohibited under the Rule.[126] Individuals must be provided notice and an opportunity to agree or object to uses and disclosures for facility directories and for patient care involvement and notification.[127] Concerning the public's health, covered entities may disclose PHI without written authorization or notice (a) where legally required; (b) for permissible public health activities; (c) to avoid serious health or safety threats to others; (d) about abuse victims in certain circumstances; (e) for health oversight purposes; and (f) for appropriate research.[128] Additional contexts lend to differing outcomes related to disclosures without written authorization, as per data examined in **Focus 2**, below.

Focus 2 – Post-Dobbs Reproductive Health Data Protections

In April 2023, HHS OCR proposed an amendment to the Privacy Rule to limit disclosures of PHI regarding lawful reproductive health care. This proposed rule was spurred by the U.S. Supreme Court's elimination of the constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization* on June 24, 2022. The premier objective was to circumvent requests for PHI disclosures from abortion-hostile states seeking to target HCPs or recipients who have provided or obtained lawful reproductive health care in abortion-protective states. The proposed amendment, which became final on April 26, 2024, does not affect routine public health data sharing. Washington's own reproductive health shield law disallows data sharing with states seeking to investigate or prosecute lawful reproductive health services or otherwise gain such information for non-health purposes.

Data disclosures pursuant to the Privacy Rule are generally restricted to the minimum necessary to accomplish the purpose of disclosure, which is echoed by the Washington Supreme Court in *Peninsula Counseling Center v. Rahm* (1986), upholding psychiatric data sharing practices via confidential, centralized, minimally-identified state records.[129] Covered entities are entitled to rely on a PHA's request for public health data as already satisfying the minimum data necessary requirement.[130] Additionally, the Privacy Rule allows covered entities to more freely disclose information via limited data sets (for which specified direct identifiers are removed), for "the purposes of research, public health, or health care operations."[131] These data sets may be disclosed upon execution of a DUA with the recipient.[132] **Figure 8**, below, illustrates key questions to consider in PHE disclosures pursuant to the Rule.

Figure 8. HIPAA Privacy Rule Flowchart[133]



Numerous additional federal information privacy laws, many of which predate the HIPAA Privacy Rule, reflect similar principles, or protect specific health data in key settings within the universe of privacy protections (see **Figure 6**, above). Select examples of federal health information privacy laws are briefly illustrated in **Focus 3** below.

Focus 3 – Additional Federal Health Information Privacy Laws

- Public Health Service Act (1944) protects information collected by federal health agencies, including HHS and NCHS.
- Freedom of Information Act (1966) protects medical and similar files held by federal agencies from acquisition via public records disclosure.
- Title X Confidentiality Requirements (1970) protect the confidentiality of patients seeking Title X-funded family planning services.
- FERPA (1974) protects educational records, including health information, prohibiting disclosure of personally identifiable information without written consent, subject to limited exceptions including for health and safety emergencies.
- Privacy Act (1974) protects identifiable data collected by the federal government and prohibits disclosures without consent absent exceptions, as per accompanying HHS Privacy Act Regulations (1975).
- Americans with Disabilities Act (1990) requires employers to protect employees' disability-related health information.
- E-Government Act (2002) limits the use and collection of health and other identifiable data for statistical purposes under its sub-titled Confidential Information Protection and Statistical Efficiency Act.
- Genetic Information Nondiscrimination Act (2008) bars disclosure of genetic information by covered entities pursuant to the HIPAA Privacy Rule.
- HITECH Act (2009) incentivizes HCPs to utilize electronic health records and requires business associates to adhere to the HIPAA Privacy Rule.
- Substance Use Disorder Patient Records (2017) requirements protect the confidentiality of individuals receiving SUD care at specific federally-funded programs.

Additional ongoing efforts in Congress seek to expand existing privacy protections to broader arrays of personal data, as well as health information specifically. For example, the Upholding Protections for Health and Online Location Data Privacy Act of 2023 sought to prohibit the use and sale of PHI and location data for advertising purposes.[134] The American Privacy Rights Act of 2024 proposes national data protection standards for information, including IHI, held by multiple industries and other settings outside typical coverage under the HIPAA Privacy Rule.[135] To date, these proposals have not been enacted.

3. Washington State Public Health Data Privacy Laws & Policies

Washington's Uniform Health Care Information Act specifies health information disclosure and access provisions, resonating the HIPAA Privacy Rule.[136] This includes a

general requirement to obtain patient authorization before sharing PHI unless specifically allowed under Washington State law or the Rule.[137] Washington State law also requires health insurers to implement policies to protect the privacy of PHI.[138] Disclosures without patient authorization are expressly allowed when necessary to protect public health.[139] The law, while containing many provisions which specifically target HCPs, was passed with the express legislative consideration that "a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than [HCPs]."[140] Consequently, Washington state agencies receiving impacted data are statutorily required to establish regulations for "record retention, destruction, and security" consistent with the UHCIA.[141] Unlike the HIPAA Privacy Rule, Washington State law allows private causes of action for individuals to enforce its provisions and recover actual damages.[142]

Supporting policies issued by WA DOH address confidential data, imposing expectations of, and procedures for, lawful handling by employees, staff, volunteers, and assignees.[143] WA DOH policies and procedures also outline permissible releases of information for public health, licensing and regulation, research, or other purposes outlined in DSAs.[144] Washington State law requires execution of DSAs to share category 3 or higher data, empowering WaTech to set flexible, state-wide policies related to this type of data (see **II.C.1**, **III.B.3**).[145] Washington law also requires WA DOH to ensure that program managers receiving health information, acting as primary data stewards, must "assure health information is protected consistent with applicable law and agency privacy, confidentiality and security policies, standards, and practices" (see **III.B.2**).[146]

In April 2023, Washington Governor Jay Inslee signed the My Health My Data Act (MHMDA), a far-reaching law expressly aimed at protecting health privacy even beyond covered entities traditionally subject to the HIPAA Privacy Rule.[147] MHMDA specifically protects consumer health data.[148] Among other provisions, it requires businesses attempting to collect, use, or share such data to:

- provide explicit notice to consumers;[149]
- obtain consent for the sale[150] or collection and sharing of the data beyond that needed to provide services to the consumer, reflecting and broadening the HIPAA Privacy Rule's requirement of valid authorization for data sale or marketing;[151]
- enable consumers to withdraw consent, delete their data, and confirm data uses and access;[152] and
- follow pre-set security requirements.[153]

MHMDA prohibits establishing certain "geofences" (i.e., "a virtual boundary" enabling location of consumers[154]) around health facilities for purposes of tracking, notifying, or collecting their health data. Violations of the Act may subject businesses to sanctions for unfair trade practices.[155] While MHMDA represents an expansive approach to protect consumer health data, none of its provisions apply to government agencies, tribal nations, or contracted service providers processing consumer health data on behalf of a government agency. Nor does the Act govern PHI, de-identified information, or other

information acquired or used pursuant to the HIPAA Privacy Rule or Washington State health data statutes.[156]

Even though state and local PHAs are not directly implicated by many privacy requirements of the HIPAA Privacy Rule or MHMDA, these laws can complicate the acquisition, use, and disclosure of data among those working with data who may be uncertain of their applicability. Covered entities have tended over time to adopt defensive techniques or stringent privacy approaches to avoid sharing data with PHAs for fear of violating privacy laws despite clear standards, allowances, or exceptions. Even "non-covered" entities may follow its privacy requirements out of confusion or concern over liability repercussions. Still, most privacy laws include exceptions and limitations to facilitate laudable, authorized uses of PHI for public health purposes.

Meanwhile, many "third party" applications (e.g., period tracker, mental health, or other health-related apps)[157] owned by non-covered entities utilize or collect individual health data outside of HIPAA protections. While CMS regulations require insurers to provide beneficiaries with overviews regarding health information protection and HIPAA coverage, federal rules do not make specific health privacy demands of these entities.[158] Additional persons or entities outside the Rule may be required to provide notices of health information breaches pursuant to ongoing regulatory efforts via the Federal Trade Commission.[159]

B. PUBLIC HEALTH DATA ANTI-DISCRIMINATION

Protecting health information is an inherent good for individuals and groups. Privacy breaches alone raise anxieties and contribute to adverse health behaviors among persons concerned about their private health information being inappropriately used by or shared with others. Unwarranted invasions of privacy can lead directly to unjustified discrimination. Without essential privacy protections, public and private entities with access to identifiable public health and other data may engage in discriminatory practices against protected individuals or vulnerable groups.

Federal and state health information privacy laws underscore anti-discrimination interests. Prior to the 1978 passage of the federal Pregnancy Discrimination Act,[160] for example, pregnant persons faced potential employment terminations and other restrictions. Despite federal prohibitions via the Act, cases of pregnancy discrimination in employment remain.[161] Ongoing HIV and AIDS-related stigma was exceptionally heightened in the 1980s, resulting in acts of discrimination and violence predominantly against gay men.[162] Keeping HIV/AIDS and other PHI private and secure helps protect against invidious discrimination that can have far-reaching consequences including mistrust of governmental public health actors or data acquisitions. Prior to and throughout the COVID-19 pandemic, mistrust of public and private sector use of PHI contributed to public resistance to exercises of emergency powers and concerns over discrimination tied to temporary modifications of data privacy practices.

Protecting individuals and groups from unlawful discrimination is paramount. Yet, as with privacy norms, careful balancing is needed to assure public health interventions are undertaken to assist marginalized or vulnerable groups,[163] including people experiencing poverty[164] and undocumented immigrants.[165] Insufficient data relating to social determinants of health can contribute to or exacerbate societal inequities.[166]

Washington State statutorily enshrines freedom from discrimination as a civil right,[167] including rights (among others) to:

1. obtain and hold employment without discrimination;
2. fully enjoy accommodations, facilities, or privileges;
3. engage in real estate, credit, and insurance transactions;
4. participate in commerce without boycotts or blacklists;
5. breastfeed in public places; and
6. recover damages.

Consistent with sweeping federal antidiscrimination protections through constitutional, statutory, regulatory, and other legal routes,[168] Washington State law prohibits discrimination in multiple settings and against specific groups. For example, employers in the State cannot discriminate against persons regarding hires, fires, terms, or compensation solely based on age, sex, marital status, sexual orientation, race, creed, color, national origin, citizenship or immigration status, veteran or military status, or disability status (including service dog use).[169] Health insurance and maintenance organizations may not cancel or fail to issue or renew insurance policies based on these same protected categories.[170] Information exchanged between individual patients and their HCPs is generally considered privileged,[171] except in legal proceedings regarding disability accommodation or discrimination claims.[172]

Employment protection statutes also implicate patient health data. The Keep Washington Working Act advances workers' rights and dignity,[173] ensuring that state and local entities uphold federal antidiscrimination laws, including those related to immigration or citizenship status.[174] According to Washington State AGO guidance, state health facilities have "no affirmative obligation to inquire into a patient's immigration or citizen status."[175] This information may still be obtained to verify public health and welfare benefit eligibility (e.g., via WSHCA), and is reportable to federal agencies as required by other federal laws (e.g., Medicaid statutes, Affordable Care Act). However, as per State AGO guidance, these data may not be used for immigration enforcement purposes.[176] WA DOH, WDSHS, and WSHCA are expressly prohibited from conditioning benefits on an individual's immigration status.[177]

C. PUBLIC HEALTH DATA SECURITY

While health information privacy entails individual rights, expectations, or abilities to control acquisitions, uses, or disclosures of their IHI, assuring data security is a distinct objective of federal and state laws. Protecting the security of IHI generally involves the use of technologic tools or administrative safeguards to guard data from unwarranted

access, exchanges, or breaches.[178] Maintaining data security can be an imposing challenge amid high-profile breaches of privacy contributing to discrimination, communal distrust of PHAs and their functions, and fears of potential liability (as per **Focus 4**, below).

Focus 4 – Potential Liability for Data Breaches

While potential liability of public health data handlers for data breaches lending to direct individual harms can be concerning, multiple protections ward against these claims:

- Though Washington eliminated sovereign immunity in the 1960s, only the State, and not individual employees, may be held liable.
- The State may also satisfy resulting judgments in lawsuits brought against its employees carrying out official duties.
- Specific civil lawsuits via the UHCIA target HCPs/facilities, not state agencies.
- Pursuant to the PRA, employees may not be found liable for losses generated from good faith records releases.

Liability concerns may still arise related to aggregated IHI disclosures later used to reidentify specific individuals. Successful liability claims against public health data handlers are rare for additional reasons:

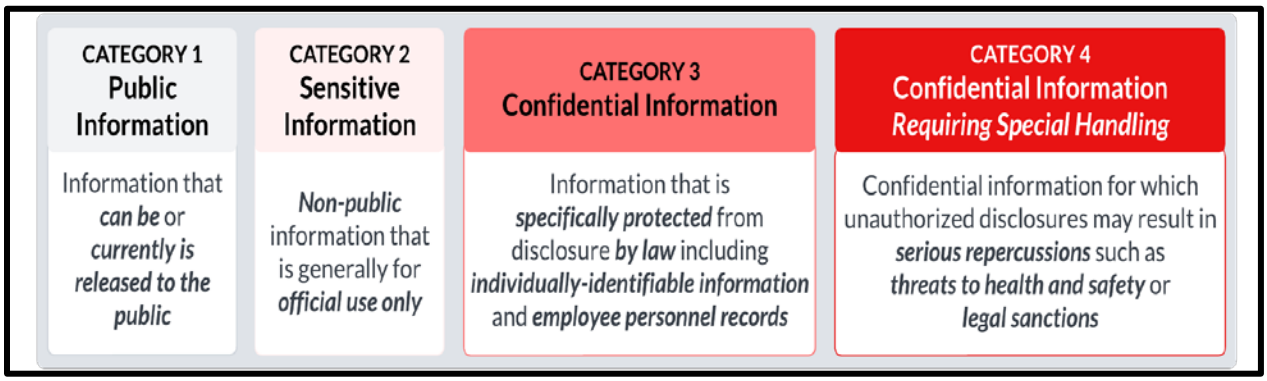
- Washington State law creates a civil cause of action for the unauthorized disclosure of private information but exempts lawful provisions of personal information "on behalf of a state agency."
- In 2008, the Washington Supreme Court rejected a privacy claim in a case involving a release of body parts and confidential records for research.
- Tort principles underlying Washington State jury instructions indicate that a separate, unforeseeable independent cause (e.g., third-party unlawful access or sharing of IHI) may shift liability away from an initial accused person or entity.
- In the event a breach is related to criminal conduct on behalf of an unrelated person, Washington State does not generally impose a "duty to protect an injured party from harm caused by the criminal acts of third parties."

1. Data Controls

A bevy of federal and state laws require varied measures designed to assure data security against the backdrop of constant threats of hacking or misuse. Pursuant to the HIPAA Security Rule, for example, certain security measures are required to avoid inadvertent access or unauthorized use of PHI. Generally, covered entities must protect against unwarranted disclosures of PHI or threats to the data.[179] Protections include limiting access to workplaces, use of encryption,[180] designation of a security officer, and workforce training.[181] WA DOH follows NIST standards for information security,[182] as well as its own data security requirements, including encryption and appropriate storage locations.[183]

WaTech oversees state network cybersecurity.[184] Pursuant to legislative direction,[185] WaTech regulates security based on 4 primary data categories: (i) public, (ii) sensitive, (iii) confidential, and (iv) confidential with special handling (see **Figure 9** below).[186] The PRA permits disclosures of "public records"[187] pursuant to specific identifiable requests (i.e., no blanket requests).[188] While public records containing category 1-2 data are subject to public disclosure,[189] category 3-4 data (which include IHI)[190] are not (see **III.B.1**).

Figure 9. WaTech Data Disclosure Categories[191]



Agencies in Washington State are tasked with ensuring data, systems, and networks remain secure,[192] including classifying categorical data consistent with their agency missions.[193] They must encrypt workstations and data, use approved algorithms for category 3-4 data,[194] and report cybersecurity data breaches to OCS.[195] Use of AI technologies in public health practice raise additional security concerns in absence of national governing mechanisms.[196] WaTech guidelines encourage "purposeful and responsible use" of AI technologies via a framework approach addressing multifarious safety and ethical concerns including data bias, cybersecurity risks, and technology misuses.[197]

2. Public Records[198]

Washington state and local agencies receiving protected data are statutorily required to develop policies regarding data acquisition, retention,[199] destruction, and security, which must be displayed on the agency's website.[200] The Public Health Records Retention Schedule, issued by the Office of the Secretary of State, specifies retention requirements for public health records of local government agencies. Records must be retained for minimum periods and then are "strongly recommend[ed]" for destruction, except for "Archival (Permanent Retention)" records.[201] For example, WA DOH HIV test reports are to be retained for 2 years and then destroyed. The Schedule aligns with the Local Government Common Records Retention Schedule, which authorizes public records transfers common to all local government agencies.[202] Additionally, per the Washington Court of Appeals in *Planned Parenthood v. Bloedow* (2015), PRA does not allow disclosures of health-related data that HCPs have shared with WA DOH pursuant

to RCW § 43.70.050 where the provider or patient can be identified.[203] Following *Bloedow*, the Washington legislature enacted a statute generally exempting from public records disclosure any health care information reported to PHAs under state law reporting requirements, compliance assessments, or for licensing purposes.[204] Pursuant to *Seattle Children's Hospital v. King County* (2020), WA DOH may have discretion relating to implementing HIPAA de-identification before releasing data where state statutes are otherwise silent.[205] PRA also does not protect against disclosure of all data. With respect to employee related records, the Washington Supreme Court has held that PRA and the state constitution do not provide a privacy interest in employee names and birth dates.[206]

3. Data Agreements & Security

In Washington State, data owners, stewards, and custodians (see **III.B.2**) overseeing specific data collections are entrusted with the protection of public health data under "applicable law and agency privacy, confidentiality, and security policies, standards, and practices."[207] These agents may be involved in implementing agency IT security standards for internal and external partners by ensuring secure interactions, closing unauthorized pathways, preventing IT hardware and software misuse, and maintaining accountability and compliance.[208] They also oversee exchanges of data through DSAs (see **III.B.3**), as well as confidentiality agreements in applicable research settings (see **I.B**).

WA DOH and other state agencies are statutorily required to rely on DSAs to set conditions for data sharing with contractors[209] and other external entities[210] concerning category 3-4 data (see **Figure 9**, above).[211] Those requesting access to confidential or restricted datasets must be approved by the data owners or delegates (see **III.B.2**). Approval processes restrict access to those with a departmental or research need for the data and correspondingly understand analytic and quality control processes, standards, or restrictions. These external agreements include explicit provisions focused on protecting data security such as:

- business, IT security, and privacy contact names and information;
- specifications including limitations for information use;
- safeguarding information requirements (e.g., small numbers guidelines, access and use limitations, responsibilities, notification, confidentiality, security, breach notifications); and
- information re-disclosures and attribution.

DSAs executed within WA DOH in support of interdepartmental data sharing are not required by law, but when utilized tend to feature fewer security measures while clarifying data specifications and persons with access.

III: NAVIGATING PUBLIC HEALTH DATA SHARING PRACTICES

Successfully navigating public health data sharing in Washington State implicates specific legal and policy requirements relating to certain types of health data and inter-jurisdictional exchanges. While various federal and state laws outline basic principles for health information privacy, anti-discrimination, and security (as examined in **II**), additional laws govern sharing particular types of public health data, often involving certain conditions, populations, and entities. Understanding the role of data agreements and specific personnel underlying inter-governmental and extra-territorial data exchanges enables more collaborative public health responses.

A. SPECIFIC DATA REQUIREMENTS

Lawful data sharing depends on the kind of data at issue. Specific health conditions, for example, may be subject to distinct protective laws or policies. Data gathered from or about certain populations, including minors, may implicate additional considerations and protections. Entities (e.g., HCPs, hospitals, SUD treatment facilities) may face separate requirements. While the diversity of Washington State laws addressing condition-specific, population-specific, and entity-specific data sharing all prioritize health information privacy and security, the sheer variety of laws and policies can complicate efforts to efficiently and effectively exchange data to accomplish public health goals. This may be especially true within WA DOH which is statutorily organized around a goal of decentralized authority coupled with "clear accountability," among other objectives.[212]

1. Condition-Specific Data Requirements

Condition-specific data protections ensure privacy of especially sensitive health data. The HIPAA Privacy Rule grounds its protections in a uniform definition of PHI that does not distinguish types of health data. State laws providing greater privacy protections or requirements for specific health data are not directly preempted by the Rule (see **II.A**). Consequently, multiple states provide enhanced privacy or other data protections that exceed the Rule. Washington State is no exception.

Numerous specific conditions or data types receive special treatment under Washington State law. Among the more prominent examples are fetal death data for vital records releases,[213] cancer data,[214] behavioral health data,[215] reproductive health services data,[216] STI data,[217] trauma data,[218] and substance use data.[219] WA DOH, for example, may release fetal death data with direct identifiers for research purposes so long as WSIRB approves and the research entity signs a confidentiality agreement (see **I.B**).[220] WA DOH may share the same information for "nonresearch public health purposes" with a governmental agency upon execution of a written DSA.[221] Patient hospitalization data including direct and indirect identifiers can only be disclosed (i) to governmental agencies at the federal, state, and local levels when accompanied by a DUA or other documentation, or (ii) for research when WSIRB agrees and a confidentiality agreement is signed.[222]

Additional requirements may apply to data relating to certain conditions, like cancer, mental health, abortion, or SUDs. Data obtained pursuant to the state's cancer registry may be broadly utilized "for statistical, scientific, medical research, and public health purposes."[223] As in most states, mental health data are viewed as super-sensitive, and thus can be disclosed without informed consent only under limited exceptions, including to courts, law enforcement agencies, and to agencies including WA DOH.[224]

Under current regulations, WA DOH and WSIRB must not publicly disclose abortion information which identifies persons without their consent, unless subpoenaed.[225] Washington State law also restricts reproductive health information shared via out-of-state subpoenas[226] (see also **II.A. Focus 3**). With respect to SUDs, Washington and federal law protect against disclosure of confidential records relating to diagnosis and treatment.[227] A recent statute requires WSHCA to develop a database in support of SUD programs.[228] Additional information on federal privacy rules impacting SUD programs is discussed in **Focus 5**, below.

Focus 5 – 42 C.F.R. Part 2 & Hospitalization Data

42 C.F.R. Part 2 protects the confidentiality of SUD data to avoid disincentivizing treatment extending from patient concerns over potential criminal prosecution or discrimination. Federally funded entities which directly engage in SUD treatment, diagnosis, and referral, including hospital units and staff devoted to these purposes, must abide by the rules and protect against unauthorized disclosure of SUD data without explicit patient consent absent a specific exception.

Despite strict privacy requirements, the rules expressly aim to carve out and fully enable "research, treatment, and evaluation" activities. Entities, including state and local governments, engaged in auditing, evaluation, and research can obtain SUD data without patient consent pursuant to Part 2 exceptions. Auditing and evaluation activities include ensuring effective resource administration and altering policies or programs to "improve care and outcomes for patients with SUDs . . . treated by part 2 programs." Updates to the rule in 2024 allow disclosure of de-identified data for "public health purposes" to PHAs consistent with HIPAA Privacy Rule de-identification requirements.

Notwithstanding legal variations underlying data sharing for precise conditions, several key trends emerge from existing WA DOH assessments:[229]

a. A broad swath of authorities permits WA DOH to collect vast amounts of distinct PHI across the state.[230] These authorities enable WA DOH data collection for public health purposes, but key uses for these data (research, collaboration with other state, tribal, or local PHAs) require that the Department be able to share them more widely.
b. WA DOH may withhold considerable public health data from public records requests[231] pursuant to state-based privacy and confidentiality protections.[232]

c. WA DOH is empowered to release much of these data for justifiable reasons including for research purposes,[233] public health activities,[234] and clinical care and coordination.[235]
d. Public health data may also be shared via public release for transparency and educational purposes, subject to additional restrictions including aggregation requirements or withholding of identifiable information.[236]

In sum, WA DOH is broadly authorized to share data for public health and research-related purposes across a variety of distinct data types despite complications stemming from diverse laws. Some statutes, particularly those relating to disclosure of data for research, require confidentiality agreements before sharing data.[237] Washington State laws expressly addressing DSAs for category 3 and 4 data are examined in more detail in **III.B**, below.

Additionally, while many State statutes support data sharing, permissible justifications are not always delineated (e.g., sharing for "public health" purposes without defining the same).[238] Finally, while some legal provisions clearly define specific direct and indirect identifiers for purposes of data disclosures, others do not. Variations and resulting amorphousness allow for distinct interpretations across different kinds of data and between data owners, stewards, and custodians (see **III.B.2**), obfuscating uniform approaches.

2. Population-Specific Data Requirements

Distinct data protections in Washington State also concern specific populations, including minors, immigrants, and indigenous persons. For example, under Washington State law, parents can access confidential records concerning their children from WDCYF. In some cases, however, children must consent to such disclosures, including (a) abortion and birth control records,[239] (b) mental health and SUD records if over age 13, and (c) STI records if over age 14.[240] Minors' mental health information can only be disclosed to "public health officers as necessary to carry out the responsibilities of their office"[241] or where public safety is implicated.[242] Similar consent requirements apply to WDSHS records.[243]

Disclosures of undocumented immigrants' health data may be shaped by the type of information collected, lending to considerations of whether collecting immigration-related information at all is prudent.[244] As noted in **II.B**, Washington AGO guidance in 2017 generally recommends against collecting immigration-related information due to federal reporting requirements.[245]

Concerning minoritized populations in Washington State, WA DOH is statutorily required to collect and share population health data potentially related to "chronic and infectious diseases, maternal birth complications, preterm births . . . hospital community health needs adjustments" and "other relevant health data" to develop projects in targeted statewide zones with "measurable and documented health disparities and poor health outcomes."[246] State agencies providing counseling, advocacy supports, or shelter for

domestic violence survivors are prohibited from disclosing information about recipients. They can only share identifiable information with the survivor's written authorization or via legal disclosures pursuant to court orders or in aggregated, unidentified formats to satisfy reporting and evaluation requirements.[247]

Several data sharing considerations arise concerning indigenous populations in Washington State. WSHCA must share information relating to psychiatric evaluation, treatment, and bed use for AI/AN populations with tribes, urban Indian health programs, and the American Indian Health Commission.[248] While public health data sharing is permissible under Washington statutes (see **III.A.1**), tribal stakeholders have previously reported difficulty in collaborating and obtaining timely access to data.[249]

3. Entity-Specific Data Requirements

Specific entities may also trigger data sharing requirements under Washington State law. After hospitals report specific patient discharge data to WA DOH via CHARS (see **I.A**), for example, WA DOH can share these data with other agencies for public health purposes and with researchers, subject to executed confidentiality agreements or DUAs.[250] As discussed in **III.A.1**, mental health services providers may release patient information under specifically identified circumstances, including to WDOC personnel and to WDSHS and WSHCA for program evaluation.[251] WDOC may disclose mental or behavioral health information to other state agencies for public safety purposes, as well as "transition, treatment, and supervision services."[252] SUD treatment facilities must provide records to WDCYF to investigate neglect and child abuse.[253]

B. DATA SHARING PRACTICES

The scope and variation of Washington State legal requirements for the sharing of public health data contribute to complex interjurisdictional and extra-territorial arrangements entailing multiple procedures across numerous persons and entities. As briefly assessed below, assuring data exchanges across governmental levels through data owners, stewards, and custodians under varying agreements present significant legal, policy, and practical challenges. The resulting web of legal requirements can ensnare requests for data exchanges, obfuscating access to information essential to protect the public's health.

1. Levels of Data Sharing

Public health data sharing varies across levels of government (e.g., federal, state, tribal, local) in Washington State, with each level claiming entitlement to specific information while simultaneously being obliged to divulge or disseminate its own. Data exchanges across governmental levels are thus a "two-way street." For example, state-level PHAs like WA DOH need key surveillance data from LHJs, who in turn seek WA DOH's public health information for their own initiatives or interventions. Dilemmas arise when different levels of government justifiably claim such data to further the public's

health, but legal logjams or practical impediments block or delay their access, use, or disclosure.

Federal requests of public health data through HHS, CMS, CDC, IHS, or other agencies to state-, tribal-, or local-level PHAs in Washington State may be legally authorized through several routes. To the extent that federal PHAs seek aggregate, non-identifiable information, they do not implicate most federal or state privacy or security laws. When identifiable data are sought, federal agencies may rely on explicit federal statutory or administrative laws sustaining their requests. For example, WA DOH may share select information received through RHINO with CDC's NSSP.[254] Federal PHAs may also craft their own DSAs with lower-level agencies as a condition of receipt of federal public health funds or resources. CDC is developing a "Core DUA" to help unify national data exchanges through its Office of Public Health Data, Surveillance, and Technology in 2024.[255]

Despite manifold federal paths to lawfully acquire data, problems emerge. State- or local-PHAs may contest data sharing requests or attempt to set procedural or other conditions of their own notwithstanding the preemptive nature of specific federal laws or funding arrangements which may mandate data disclosures. State, tribal, or local PHAs requesting some health data or analyses from federal sources may experience federal reticence on privacy law or policy grounds.[256] Federally-supported SUD treatment centers, for example, view their data as super-sensitive under federal administrative law, disallowing requests for data about their patients even in the interests of public health promotion (see **III.A.1**).

State-level data exchanges can be equally complex. As noted in **II.A**, Washington statutory laws require state agencies to execute written agreements in advance of sharing category 3 or higher data.[257] In reality, legal misalignments of state agencies under extant privacy standards or expectations hinder cross-agency data sharing. In most cases, sharing confidential data within these departments can be negotiated through execution of DSAs or DUAs, but at considerable time and expense, and subject to controversy as discussed in **Focus 6** below.

Focus 6 – State-to-State Public Health Data Sharing

States routinely request public health data related to specific conditions or treatments from neighboring states where residents have received care. However, each state's unique methods and procedures for data exchanges and uses may not align. In 2023, for example, the medical director of a nearby state's communicable disease program requested data about a number of residents from that state who were hospitalized in Washington. Data sharing was stalled as Washington health authorities attempted to negotiate a DSA with corresponding public health partners in the nearby state. As per this example, stringent requirements for data agreements can strain relationships, impede legitimate data flows, and impact public health interventions. Additional insights on political and social factors involving sharing of abortion-related information are examined in ***Focus 3***.

State-to-state public health data sharing can be tricky, but such exchanges between state and tribal PHAs in Washington State can be even more complex. As distinct sovereign entities within state borders, tribal PHAs present unique legal and policy issues. State agencies in Washington are statutorily required to "[m]ake reasonable efforts to collaborate with Indian tribes in the development of policies, agreements, and program implementation"[258] including on matters of public health and safety.[259] Securing data exchanges between state and tribal PHAs can be underwritten through agreements and procedures as per state-to-state or state-to-local exchanges. However, uniformity is critical to expedite sharing across and between the 29 tribal governments within Washington State borders.[260] WA DOH is developing a single prototype DSA to apply to most data sharing requests between the Department and tribes.

LHJs in Washington State are beholden to follow state public health laws and policies, notably including adherence to public health surveillance and other data sharing requirements applicable to WA DOH (see **I.A** & **II.A**). LHJs are also statutorily allotted a level of "home rule" authorities to "[e]nact such local rules and regulations as are necessary in order to preserve, promote and improve the public health . . . ."[261] Consequently, they are both "givers" and "seekers" of IHI at the federal-state levels, and across their jurisdictions.[262] Larger LHJs like Seattle-King County have explicit public health data needs for which they may stake claims to state-based data uniquely gathered by WA DOH (e.g., HIV/AIDS, opioid use information). Conversely, state PHAs rely extensively on LHJs to regularly exchange identifiable information for a plethora of public health needs. As with other data practices, in many cases these exchanges are negotiated via agreements by data handlers whose roles are delineated below.

2. Roles of Data Owners, Stewards & Custodians

Even when data exchanges across governmental levels or outside of specific agencies are warranted, executing them falls to a triumvirate of information specialists categorized by WA DOH (and other state agencies) as data owners, stewards, and custodians. Within various state PHAs, these persons ideally serve distinct roles undergirded by their perceived or actual need to adhere to strong privacy and security protections. In reality, the functions of these agents are not wholly independent even under WA DOH guidance designed to clarify their distinctions. The capacity for overlapping responsibilities, strict interpretations, gate-keeping requirements, or untimely execution of DSAs or DUAs (see **III.B.3**, below) among these personnel can delay or derail essential data exchanges.

Data owners are characterized via WA DOH guidance as senior-level health officials who are broadly accountable for public health information in specific data areas (e.g., STIs, injuries, chronic conditions). They oversee and authorize data stewards who are SMEs responsible for data management on a daily basis. Stewards are delegated by data owners the authority to "acquire, create, maintain and protect electronic information."[263] Where stewards are responsible for content, custodians oversee safe data holding, transport, and storage through technological or other means.[264] In sum,

owners are the lead officials, stewards are the data managers, and custodians are the information technologists.

When the roles and responsibilities of these agents mesh well, public health data sharing in Washington State within WA DOH and other agencies routinely occurs in line with privacy and security protections. When these distinctions are clouded or specific agents' roles or interpretations diverge, complications and breakdowns of exchanges can arise. To the extent that each of these personnel have competing responsibilities as gatekeepers of data, their capacities to negotiate specific practices, limit data access, and report potential security violations can impinge legitimate information sharing, triggering actual or perceived breaches or legal limitations.

3. Data Sharing & Use Agreements

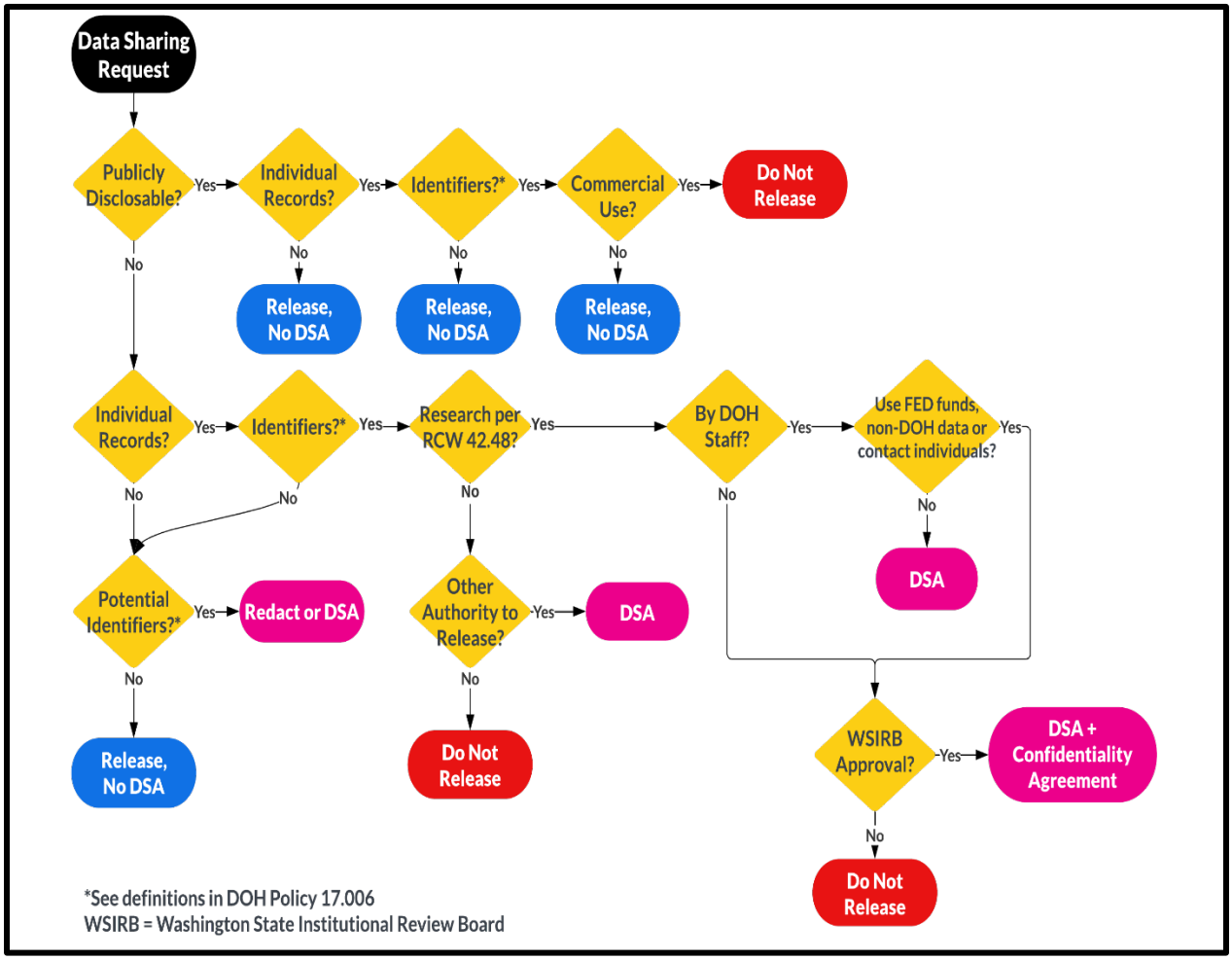
Underlying inter-governmental and extra-territorial public health data sharing through owners, stewards, and custodians are explicit legal requirements pursuant to a prevailing "culture of confidentiality" to execute DSAs, DUAs, or other agreements effectuating data exchanges.

As indicated previously in **II.A.3** and **III.A**, Washington State law expressly requires execution of DSAs and DUAs for many reasons when data are shared, including for research and public health purposes. While some statutes refer expressly to written "data-sharing agreement[s]," and other statutes require signed "data use agreement[s],"[265] WA DOH views DSAs and DUAs as largely equivalent.[266] Beyond exchange-specific DSA/DUA requirements illustrated in **II.A**, Washington laws and policies[267] set broader procedures for sharing data internally and externally. Washington State agencies seeking to share category 3-4 data with contractors,[268] for example, must have "a written [DSA]. . . in place" satisfying WaTech policies.[269] Some exceptions arise in the event of known public health threats (e.g., COVID-19) when minimum data needed to avert or respond[270] may be shared upon a waiver of existing DUAs.[271] WaTech has published a number of guidance documents, including general language which may be included in DSAs to address distinct issues.[272] Despite this and other guidance, concerns regarding the permissible breadth and scope of DSAs for certain audiences or groups remain paramount.

At the heart of many challenges regarding data exchanges in Washington State may be recent amendments to the state's Interlocal Cooperation Act which require stringent DSA implementation for data exchanges without exception for public health data uses.[273] Public agencies[274] (including municipalities, tribes, and state and federal agencies) requesting category 3 data or higher from each other must provide "for a written agreement between the agencies" (see **Figure 10**, below).[275] These data categories, initially discussed in **II.C.1**, are not prescribed via legislation or regulation, but rather via WaTech policy.[276] State or local agents attempting to negotiate or follow these policies can experience complications or misunderstandings. A lack of statewide standardized identifiers lends to disagreements among data stewards regarding aggregation methodologies or techniques which can hinder timely and accurate data exchanges.[277]

WA DOH utilizes standardized internal and external[278] DSA templates to effectuate data sharing. In addition to security and confidentiality requirements, the internal template requires, "as necessary," specific descriptions of data to be shared, including database identifiers, elements, formats, and time frames. Initial or subsequent WA DOH staff accessing public health data must also sign the agreements. Although execution of internal DSAs are not legally-required for exchanges of health data within WA DOH, they may still be utilized for documentation purposes to track approval and access to specific data.[279] Additional specifications arise within DSAs authorizing external sharing with persons or entities outside WA DOH. Although Washington State laws do not adopt a universal approach to direct and indirect identifiers, the external template specifically defines these terms. The template further requires that data be stored within the U.S., enables immediate termination upon unauthorized data uses or disclosures, and requires the data requester to "strictly limit" use of the data subject to purposes expressly illustrated in agreement exhibits. These exhibits require detailed purposes for data, data descriptions, statutory authorization, access methods, and data disposition certification.[280]

Figure 10. WA DOH Flowchart – When a DSA Is Required[281]



IV: PATHS TO IMPROVED PUBLIC HEALTH DATA SHARING

In numerous ways, the laws and policies underlying public health data sharing in Washington State reflect model approaches balancing essential data acquisitions, uses, disclosures, and security. Core values underlying these exchanges – the common good, accountability, transparency, and equity – are reflected in the State's practices of protecting health information privacy, preventing discrimination, and avoiding security breaches.

Beyond privacy, universal data sharing principles reflect additional goals. To the degree these data are lawfully and ethically collected and used to improve public health outcomes, they advance a quintessential societal objective. ***Acquiring PHI for public health purposes is a legitimate public good.***[282] The Washington State legislature has recognized unequivocally that "development and maintenance of adequate health care information, statistics and projections of need for health facilities and services [are] essential to effective health planning and resources development."[283] To this end, extensive use of such data to improve public health outcomes is highly appropriate and essential. Failing to acquire and use such data for public health purposes diminishes the community's health, especially through governmental PHAs bestowed with lawful authorities and duties to protect it.

Finding the perfect balance between allowing public health data acquisitions and uses and protecting privacy, anti-discrimination principles, and security can be difficult. Misbalances on either side of the scale lend to perverse results – reckless data sharing and breaches at one extreme; de-minimized data uses and overly-restrictive policies at the other. Neither outcome is acceptable given the demonstrated synergies between promoting the public's health and protecting privacy (see **II**). Enabling PHAs to acquire and use public health data fully without impinging individual privacy or breaching security is key.

Affirmative policies resonating these principles bode well for a state like Washington whose unquestioned commitment to public health and safety is legally-supported. Protecting the public's health means a lot to Washingtonians and their state and local PHAs. To the extent their data sharing policies allow timely, accurate, and responsible uses of properly acquired public health information, whether identifiable or not, legal or policy adjustments are not needed.

Conversely, when data laws or handlers invoke overly restrictive or defensive information approaches or policies, they embroil PHAs and their partners in needless, costly, and sometimes inhibitive efforts. These complications slow the dissemination of needed information or strip away key components of data sets. Worse yet, purposeful data exchanges may be voided altogether. This is untenable. ***No one's preventable and poor health outcomes should be owed directly to failures to share meaningful public health data legally and responsibly*.**

A. SCOPING THEMES

Several key themes of potential changes, shifts or reforms in public health data exchange practices or procedures are explained below. These themes are based on (1) research, analyses, and assessments within the Report (with cross references); and (2) global or domestic information practices improving public health data flows while respecting individual privacy and data security.[284] Following each subsection is an "**illustration**" of how the theme resonates in Washington State. Implementation of legal reforms or changes in policies or practices based on these themes or others rests with law- and policy-makers in Washington State.

1. Equality of Access Across Governmental PHAs

Like most states, Washington State public health data sharing laws allow significant acquisitions of PHI for surveillance, investigations, research, and other purposes (see **I**) shared across state, tribal, and local PHAs. What these agencies do not share, however, is equal access to key public health data they need to effectuate their objectives. Ideally, PHAs should enjoy a presumption of access upon demonstrating their interjurisdictional requests for data are legitimate and purposeful.[285] Washington's approach may be more stringent than other states, which do not require such a heightened level of data management. Some other states take broader data sharing approaches. Illinois, for example, recently passed the Access to Public Health Data Act, expressly requiring certain state agencies to disclose residents' public health data to LHJs.[286] So long as the data stay within the bounds of appropriately entitled PHAs, their capacity to assure the privacy and security of the data is strong, as is their accountability.

Illustration: WA DOH obtains a vast amount of different data from HCPs across the state largely through legal interpretations of state or federal law permitting disclosures (typically without informed consent) (see **II**). Yet LHJs may face difficulties in subsequently obtaining access to these data from state agencies, even where interpretations arguably permit data disclosures to localities in similar circumstances. Tribal governments have expressed similar complications in obtaining health data, leading to long-standing efforts to implement a broad DSA between state government agencies, tribes, and tribal epidemiology centers.[287] ***All PHAs should enjoy presumptive access to data for legitimate public health purposes.***

2. Establishing Legitimate Public Health Purposes

Allowing equal access of public health data across state, tribal, and local PHAs presupposes a consistent justification for the data.[288] The Model State Public Health Privacy Act (MSPHPA) defines sufficient "public health purposes" warranting data exchanges. Specifically, a "legitimate public health purpose" is a:

> "population-based activity or individual effort primarily aimed at the prevention of injury, disease, or premature mortality, or the promotion of health in the community, including (a) assessing the health needs and

> status of the community through public health surveillance and epidemiological research, (b) developing public health policy, and (c) responding to public health needs and emergencies."[289]

Beyond defining the term, MSPHPA provisions allow data exchanges between and among PHAs that further these purposes, largely without extensive procedural hurdles, administrative requirements, or other unwarranted burdens. Data exchanges that do not further such purposes, however, may be subjected to considerably greater privacy restrictions, especially disclosures of data outside PHAs. The end goal is to facilitate, and not impair, data exchanges between and among PHAs (including in other jurisdictions) for legitimate public health purposes.[290]

Illustration: Statutory law in Washington includes a broad definition of "public health" referring generally to the "well-being of the general population" and "actions . . . to preserve, protect, and promote the health of the people for which government is responsible. . . ."[291] While these and other general statutes authorize state and local PHAs to perform a range of public health services and functions, the State legislature has not statutorily determined a driver of legitimacy for public health data exchanges (e.g., it has not adopted the above MSPHPA provisions). In fact, as per scoping **theme 3** below, over-layering of privacy protections across specific conditions, types of data, and data sources or recipients obfuscates exchanges further. Absent clarity as to what constitutes a legitimate public health purpose, data exchanges in the interests of the public's health in Washington State may generate divergent legal and policy interpretations.

3. De-layering Data Sharing Laws & Principles

As elsewhere, Washington State laws reflect a layered approach to protecting public health data privacy within the constraints of existing technological challenges and legal landscape. As per **II** and **III**, specific laws tied to certain kinds of data were passed or promulgated in response to actual or perceived needs for enhanced privacy. Consequently, similar data of various levels of sensitivity are treated distinctly for privacy purposes. Overlaying state laws are federal privacy laws and principles. Beneath state laws are local legal requirements among LHJs with sufficient home rule authorities. Navigating the maze of privacy laws can be burdensome, especially when actors unnecessarily use privacy protections in lieu of allowing legitimate uses. Washington State lawmakers cannot change federal privacy approaches regarding SUD treatments, mental health, or other hyper-sensitive data, but they can adapt their own laws to de-layer unwarranted privacy distinctions, preempt contrary local level laws and policies, and use (where possible) de-identified data (as suggested further below).

Illustration: Most, if not all, states address certain conditions with heightened data protections, like information relating to mental health, STIs, or minors. Along these lines, several Washington state laws distinguish condition-specific, population-specific, and entity-specific data (see **III.A**), contributing to diverse privacy and other protections attached to these data. Multiple layers of data laws can be counter-intuitive to modern

public health sharing practices assimilating protections for all public health information as espoused in the MSPHPA.[292]

4. Authorizing Public Health Data Acquisitions & Uses

Acquiring public health data is justified ethically by its responsible use to protect and promote communal health. Ultimately, public health data should be findable, accessible, interoperable, and reusable (FAIR) to improve actual public health services, other uses, and research.[293] Even after public health data are acquired, explicit allowances for uses of the data within state, tribal, and local PHAs vary extensively due to deviations among existing state laws as well as extensive reliance on DSAs whose terms may be altered significantly across entities and jurisdictions. DSAs reflect affirmative privacy protections which may be warranted for some, but not all, data exchanges. Consequently, even after public health data are lawfully acquired, their uses for legitimate public health purposes may be tied to privacy norms that exceed legal or practical boundaries. Remedying this imbalance could greatly expedite and enhance data exchanges.

Illustration: The Washington State legislature has specified a limited number of data sharing practices via statute but deferred to state or local PHAs on others. LHJ's authorities to establish their own data confidentiality protections can vary as well. The resulting jumbled information environment encourages individualized data negotiations and divergent approaches governing data uses at different levels of government and across agencies. Under the MSPHPA (see **IV.A.2**), internal uses of public health data by all PHAs are largely assimilated, allowing for freer flows of information that are uniformly protected from privacy and security infringements in any setting.

5. Standardizing Data Definitions & Identifiers

Data handlers among state, tribal, and local PHAs in Washington State struggle to authorize exchanges in part because of non-standard definitions. Key concepts like what qualifies as de-identified or non-identifiable data are left to differing interpretations given a lack of uniformity around the definition of "identifiers." The State has not incorporated the HIPAA Privacy Rule list of identifiers via reference like it has Common Rule provisions. WA DOH's detailed guidance on exchange of "small numbers" data perpetuates cross-interpretations and adverse outcomes. Differences of opinions among data handlers as to how much or little data should be shared lead to delays or denials, which could be relieved to some extent if specific data terms were clearer. Increasingly, public health data practices are considering standards that distinguish between direct and indirect identifiers. Emerging data principles would thus limit exchanges of data with direct identifiers that immediately denote specific persons (as reflected in multiple Washington state laws) while allowing greater exchanges of data with indirect identifiers (i.e., "pseudonymized data") that cannot.[294] Additionally, identifiable data should be assumed to be able to be linked for legitimate public health purposes.

Illustration: Washington State laws sparingly illustrate express identifiers, doing so with respect to select kinds of data like vital records release data or CHARS information (see **I.A**). To the extent these identifiers are tied expressly to key data sources as per state law, exchanges of other data are subject to differing interpretations regarding identifiers. Disagreements among PHAs about how to effectively de-identify data can stall transfers of information or implicate distinct jurisdictional policies, potentially causing loss of meaningful data along the way. Select approaches via DSAs may ultimately favor privacy concerns over public health needs.

6. Clarifying Disclosures & Secondary Uses

Privacy is paramount when public health data leave the boundaries of PHAs. In other states and as per principles espoused in the MSPHPA, data "uses" are distinct from "disclosures."[295] Uses of PHI for legitimate public health purposes within state, tribal, or local PHAs governed under uniform privacy laws are largely allowed without significant state-level oversight. So long as PHI are held within state or local PHAs, uses may include initial, intended purposes justifying their acquisition as well as secondary, or downstream, exchanges to accomplish additional public health objectives without strict additional levels of review.

Only when such data are disclosed outside PHAs are standard privacy protections (e.g., explicit informed consent, written authorization, and DSAs) required. Washington State law is unclear on the distinctions between uses and disclosures, which can lend to over-applications of privacy protections to all exchanges that are antithetical to public health data sharing principles and timely exchanges. Privacy concerns can inhibit public health data sharing, as evidenced via meta-analysis across multiple jurisdictions, where "clear distinction[s] between data containing personal identifiers and fully anonymous data may not always be possible, leading to restrictive policies on all types of data due to privacy concerns."[296]

Illustration: As described in **II.A.3**, Washington's UHCIA, which is largely focused on HCPs, anticipates that agencies receiving the data will establish regulations consistent with the Act's provisions. Among the Act's provisions are numerous requirements relating to "health care information access and disclosure."[297] Provisions address *disclosures* by HCPs,[298] patient-authorized *disclosures*,[299] *disclosures* permitted without authorization,[300] required *disclosures*,[301] and *disclosures* relating to certain kinds of data, including STI data[302] and mental health data.[303]

Despite its focus on "disclosures," the Act fails to accurately define the term,[304] or distinguish data "uses" from "disclosures." Actually, the UHCIA basically equates "uses" and "disclosures" as interchangeable. It prohibits, for example, HCPs from the "[use] or disclos[ure] or health care information for marketing" not permitted by federal law.[305] Banning uses and disclosures of IHI for marketing purposes makes sense from a privacy perspective, but applying similar methodology to *public health* uses and disclosures impedes communal health objectives.

7. Diminishing Role of DSAs

Heavy reliance on DSAs to authorize nearly every facet of public health data exchanges, whether expressly required by law or not, is a core facet of Washington State data sharing practices. DSAs are unquestionably warranted for some data exchanges where public health objectives or purposes are obtuse, ill-defined, or potentially absent,[306] but not for standard, routine uses of public health data within or between PHAs. Such practices frustrate internal and external partners, lending to less collaborative public health efforts overall.

Illustration: DSAs are required expressly in certain Washington statutes pertaining to specific kinds of data but are also mandated broadly with respect to category 3 and category 4 data pursuant to Washington state law and WaTech policies. For example, vital records information which includes direct identifiers may be released for research purposes with WSIRB approval and a written DSA executed by the research organization and WA DOH.[307] The same is true for research relating to CHARS data.[308] CHARS data may also be released with a signed DSA to "federal, state, and local government agencies."[309] Inconsistent applications of these and other requirements can stymie PHAs timely access to public health data. WA DOH's extensive, base-level external DSA is over 20 pages long, lending at times to difficult and protracted contractual negotiations between PHAs legitimately seeking data for permissible uses. Illinois' Access to Public Health Data Act prioritizes more comprehensive master DUAs with LHJs, presenting a potential compromise approach between executing numerous stringent, data specific DSAs and avoiding DSA use altogether.[310] Ultimately, public health data sharing between and across state and local agencies should be as unencumbered as possible with legislative support where possible.

8. Prioritizing Data Sharing Collaboration

Collaboration is a prerequisite to facilitating efficient and effective data exchanges between PHAs. Governmental requesters seeking data for "legitimate public health purposes" (see **IV.A.3**) should generate collaborative attempts to facilitate data sharing. When data requests are viewed initially as privacy risks, rather than as opportunities to achieve public health benefits, exchanges become much more difficult to accomplish in a timely and mutually beneficial manner. Moreover, approaches to data sharing, including policy development and DSA drafting, should be undertaken collaboratively and inclusively, ensuring that state, local, and tribal allies shape the data sharing environment as trusted partners. In this way, governmental entities vested in data sharing may not only help to shape state-level policy, but also ensure their own policies reflect similar, collaboratively-developed approaches, eliminating additional jurisdictional barriers to data sharing over time.

Illustration: Washington State law approaches data sharing between governmental partners from a proscriptive, rather than collaborative, approach by setting sometimes stringent DSA requirements on category 3 and above data, even between governmental actors, and without exceptions for legitimate public health exchanges.[311]

Additionally, WA DOH's internal and external DSA templates cut against collective data sharing efforts. Internal and external partners of Washington State struggle at times to efficiently obtain key data, which in turn may negatively impact trust relationships between partners and the ability to undertake beneficial public health actions. More collaborative efforts throughout the policy development and sharing process may build trust in the legitimacy of data exchanges and assurances of privacy protections.

9. Distinguishing Responsibilities of Data Handlers

Data handlers (e.g., owners, stewards, custodians) are ideally vested with distinct responsibilities to negotiate, acquire, hold, and protect public health data. Their legal roles, however, meld together through complex DSAs and contrary interpretations that can stymie or stop data flows. Streamlining access to critical data to select persons with responsibility for data management within PHAs is not the problem *per se*. Multiple privacy principles support the premise that access to sensitive data, even within PHAs, should be limited to those with a need to know. The problem is that data handlers controlling the information at times may adhere to a "culture of confidentiality" buttressed by legal needs to obviate data breaches or report them when they happen. Unmet demands to access or use data for public health purposes may result.

Illustration: Washington State agency guidance distinguishes multiple kinds of data managers, defined as data stewards, data owners, and data custodians (see **III.B.2**). Yet, their roles are seemingly overlapping. For example, pursuant to WA DOH guidance, data stewards authorize data access, while data custodians "[m]anage data access controls."[312] Additionally, while data stewards ensure good quality data, custodians operate processes to alter, change, or remove data. This suggests that an individual who has identified data that are not of good quality must defer to other authorized personnel to alter or remove it, complicating data processes. Data stewards and data custodians seem to directly share certain responsibilities, including reporting security issues and ensuring data are protected from unauthorized access.[313] These overlapping roles can complicate data sharing efforts and slow exchanges.

10. Expediting Data Flows for Emergency Purposes

As experienced during the COVID-19 pandemic, real-time access to data in emergencies is critical. Lives and livelihoods are dependent on timely data sharing with minimal restrictions as to their legitimate uses.[314] During the pandemic, Washington State PHAs found ways to rapidly communicate key data through express waivers of existing privacy legal requirements under emergency declarations. Their demonstrated capacities in emergencies to authorize real-time data exchanges may actually be a model for practices which could be adopted in or adapted for routine circumstances.

Illustration: Washington State law expressly enables waiver of certain DSA requirements in emergency circumstances, including those applicable to the sharing of RHINO data. Specifically, the signed DSA requirement for these data exchanges "must be waived for public health authorities" "[i]n the case of an emergent public health

threat."[315] Enabling a broad approach of appropriate data sharing with PHAs absent express DSAs outside of emergencies may facilitate timely and effective data exchanges.

B. SPECIFIC LEGISLATIVE OR REGULATORY REFORMS

In addition to potential approaches and associated law and policy reforms introduced and discussed broadly in the subsections above, specific reforms of statutory or regulatory provisions in Washington State may be warranted, as delineated in **Table 1**, below. Many of these reforms follow, or are consistent with, the broader numbered "scoping themes" above, as per indications of the specific themes supporting a prospective reform listed in the first column of the table. Other entries in the table present free-standing opportunities to address explicit legal issues that may hinder meaningful public health data sharing policies or practices in the State. As noted above in **IV.A**, each of these proposed reforms lies in the discretion of state law- and policy-makers.

Table 1. Proposed Legislative or Regulatory Reforms

# Scoping Themes	Proposed Legal Reform	Justification
#1 Scoping Themes 2, 3, 6	**Statutorily define "legitimate public health purposes."** Define via statute what may be deemed "legitimate public health purposes" for which identifiable or other data may be exchanged among PHAs as "uses" rather than "disclosures." Enhanced definitions entail amending various State laws that insufficiently describe when state or local PHAs may release legitimate information to protect the public's health.	Broadly-defined "legitimate public health purposes" as a standard metric may authorize expedited data uses across state and local PHAs and reporting entities without stricter, "red tape" privacy or reporting requirements associated with "disclosures" to outside parties where privacy risks are considerably greater. Sufficient definitions may also facilitate data sharing without duplicative or unwarranted additional operations.
#2 Scoping Theme 1	**Require state-local public health data disclosures.** Enact legislation similar to Illinois' Access to Public Health Data Act[316] to require disclosure of data for public health purposes between state and local PHAs.	Legislatively ensuring local access to data may better facilitate cooperation and coordination between LHJs and state agencies and enable more efficient local public health responses.
#3 Scoping Themes 2, 5	**Permit broader research data disclosures by ensuring that IRB requirements and "research" definitions match federal requirements**. Amend RCW § 42.48.010 to define "research" in line with federal definitions (e.g., 45 C.F.R. § 46.102(l)). Amend RCW § 70.02.210 to permit HCPs or facilities to disclose patient health care data for	Ensuring that Washington State policy towards HSR matches federal policy enables broader research-based activities and eliminates potential barriers. Permitting researchers to share public health research data with state agencies without strenuous confidentiality requirements or "explicit" statutory or regulatory permissions is consistent with public health data

# Scoping Themes	Proposed Legal Reform	Justification
	specific public health research purposes without extensive IRB approval. Repeal statutes (RCW § 42.48.040) requiring researchers to follow stringent confidentiality and security requirements.	policies framed around legitimate public health purposes noted above in #1.
#4 Scoping Themes 2, 5	**Clarify surveillance v. research distinctions.** Standardize general principles for classifying public health surveillance versus research through legislative delegation to WA DOH to craft or clarify definitive state-wide guidelines.	Providing uniform guidance for distinguishing public health surveillance and research will assist data handlers ascertain applicable privacy standards, avoid superfluous debates between IRBs or PHAs, and resonate with Common Rule clarifications that "surveillance" is not HSR.
#5 Scoping Themes 2, 5	**Standardize de-identification.** Specify which information must be removed from IHI to definitively qualify it as "de-identified" for all data exchange purposes.	Defining key identifiers which must be removed to de-identify IHI similar to approaches via the HIPAA Privacy Rule consistently across the state may help settle what constitutes IHI vs. de-identified data.
#6 Scoping Themes 1, 2, 3, 5	**Eliminate DSA categorization confusion.** Either repeal statutes requiring execution of DSAs pursuant to categorization of data (RCW §§ 39.34.240, 39.26.340) or amend them to allow specific exceptions where governmental actors seek to share data solely for legitimate public health purposes.	Excessive statutory DSA requirements hinging on time-consuming data categorization assessments can curtail legitimate public health data exchanges between governmental actors and partners. Removing or amending these restrictions may expedite data exchanges without significantly compromising privacy interests.
#7 Scoping Themes 3, 8	**Standardize data sharing allowances.** Modify select statutes (e.g., RCW § 43.70.545) to accommodate data exchanges with stakeholders by allowing broader data sharing practices.	Modify statutes with specific provisions for data sharing with select entities (e.g., higher education institutions for research purposes) to eliminate discrepancies among varied partners with similar or equal interests in data access.
#8 Scoping Themes 3	**Standardize data reporting procedures.** Modify reporting requirements for conditions that have been singled-out via specific statutory or regulatory reporting requirements to streamline reporting from LHJs.	Uniform reporting requirements for conditions across categories can help limit or remove administrative barriers and enhance efficiency of data reporting and subsequent public health actions.
#9 Scoping Themes 5, 8	**Standardize local surveillance practices.** Empower WA DOH to review and set uniform surveillance practices (including those specified in DSAs) for data collection and reporting.	Amend or update laws, regulations, procedures, and practices to enhance data collection, surveillance, and reporting uniformity and standardize LHJ practices for licensing, regulation, research, or other purposes.

# Scoping Themes	Proposed Legal Reform	Justification
#10 Scoping Theme 8	**Promote collaboration across reporting facilities and PHAs.** Amend laws and regulations (e.g., WAC § 246-101-605) with stringent reporting requirements to encourage collaboration between HCPs and PHAs with allowances for alternative approaches where warranted. Amendments to existing regulations may require concomitant changes to State Board of Health rules.	Collaborative data sharing approaches justify reforms of existing, divergent statutes to reduce complexities delaying or hindering data sharing, and encourage standardization between governments and reporting entities.
#11 Scoping Theme 3	**Clarify guidance on "small numbers" data sharing to comply with federal health information privacy guidelines.** Review and amend State guidance re: "small numbers" data sharing to comport with updated national definitions and procedures for statistical reporting and analysis purposes (e.g., U.S. Cancer Statistics guidelines for Suppression of Rates and Counts;[317] CDC guidelines for Public-Use Data Files and Documentation[318]) or applicable federal model DSAs.[319]	Reviewing and revising Washington State standards for reporting data with small numbers to comport with national standards or federal DSA models may reduce administrative burdens and assist data stewards and others to interpret and apply such guidance uniformly without significant liability concerns. Multiple models used by federal entities enable specific public health data analyses within protections outlined in federal laws. Conversely, greater uptake of pseudonymized data practices may obviate privacy concerns regarding exchanges of data between PHAs by replacing identifiable information with pseudonyms (e.g., "randomly-generated values") that allow for broader exchanges without explicit privacy risks.[320]
#12 Scoping Themes 4, 10	**Emergency allowances.** Amend State laws to ensure that definitions of "emergency" or "PHE" allow PHAs to share data in line with federal requests and to enhance emergency preparedness and response.	As part of State emergency preparedness and procedures, establishing special waivers and flexibilities during emergencies facilitates rapid emergency responses.
#13 Scoping Themes 3, 7, 8	**Clarify data categories.** Amend laws and policies in multiple locations in Washington statutes and regulations relating to data categories for disclosure purposes to clarify distinctions and approaches to different kinds of data.	Overlapping or unclear distinctions between category 1-4 data impede data sharing within and between PHAs including explicit circumstances warranting DSA execution. Even if existing categories are retained, consider clarifying that explicit data exchanges among PHAs for legitimate public health purposes are excepted from more stringent privacy protections.

# Scoping Themes	Proposed Legal Reform	Justification
#14 Scoping Theme 3	**Standardize public health category data disclosures requirements.** Varying privacy standards impede public health data sharing. For example, disclosures of vital records information to persons outside PHAs "must be reviewed and approved as to scientific merit and adequacy of confidentiality safeguards" (RCW § 70.58A.520) whereas trauma data disclosures must be "consistent with requirements for confidentiality of patient and quality assurances records" (RCW §70.168.090).	Amending various statutory provisions, regulations, and other guidance for specific data types will streamline data sharing and further broader goals of enhanced collaboration across and between agencies.
#15 Scoping Themes 5, 8, 9	**Clarify data steward and custodian roles and responsibilities.** Legally define and distinguish between roles and responsibilities of data stewards, custodians, and other persons with control over data storage and security.	Duplicative or overlapping roles and responsibilities of varying actors accountable for data privacy and security lends to differing practices and procedures. Statewide standardized data handling roles may facilitate data sharing and aggregation in the promoting timely and accurate data exchanges.
#16 Scoping Theme 7	**Repeal laws (e.g., RCW § 39.34.240) requiring DSAs between agencies.** Remove or amend statutory legal requirements for formal DSA agreements among State, tribal, or local PHAs prior to sharing category 3+ data in line with the concept that internal PHA data exchanges are "uses" and not "disclosures."	Consistent with the entries above, internal data sharing for "legitimate public health purposes" may be deemed data "uses" among State, tribal, or local PHAs which do not require extensive DSA executions. To the extent that existing legal requirements remain, fully pursuing "institutional" wide DSAs (currently under consideration in Washington State) can facilitate standard public health data exchanges, including respect for tribal nation data sovereignty.
#17 Scoping Theme 7	**Incorporate via reference regulatory guidance re: a template for DSAs.** Existing Washington state statutory laws allow significant discretion (in most cases) as to the content and scope of DSAs. In lieu of requiring extensive and complicated boilerplate provisions in each DSA, identify and publicize standard language administratively (which such documents can then defer to expressly, focusing more so on dispositive provisions).	By simplifying, publicizing, and incorporating via reference boilerplate language of any DSA executed in Washington State, resulting documents may be streamlined, allowing for considerably more rapid reviews and execution that in turn can lower administrative burdens for DSA signatories without compromising privacy or significantly risking legal liability.

REFERENCES

[1] WASH. REV. CODE § 43.70.005.
[2] WASH. REV. CODE § 43.70.512.
[3] WASH. REV. CODE § 43.70.515.
[4] WASH. ADMIN. CODE § 246-101-005.
[5] Peter Nsubuga et al., *Public Health Surveillance: A Tool for Targeting and Monitoring Interventions*, *in* DISEASE CONTROL PRIORITIES IN DEVELOPING COUNTRIES (2d ed., 2006).
[6] JAMES G. HODGE JR., PUBLIC HEALTH LAW IN A NUTSHELL 263 (4th ed. 2022).
[7] WASH. REV. CODE § 43.20.050.
[8] WASH. REV. CODE § 43.70.057.
[9] WASH. REV. CODE § 43.70.052.
[10] WASH. REV. CODE § 43.70.545.
[11] WASH. STATE DEP'T HEALTH, WASHINGTON DISEASE REPORTING SYSTEM: REFERENCE GUIDE (2017).
[12] WASH. STATE DEP'T HEALTH, WASHINGTON DISEASE REPORTING SYSTEM: REFERENCE GUIDE (2017).
[13] WASH. REV. CODE § 70.02.050.
[14] WASH. ADMIN. CODE §§ 246-101-120, -230, -515, -610.
[15] *Syndromic Surveillance (RHINO)*, WASH. STATE DEP'T HEALTH.
[16] WASH. REV. CODE § 43.70.057.
[17] *Syndromic Surveillance (RHINO)*, WASH. STATE DEP'T HEALTH.
[18] *Washington State Public Health Data Exchange Eligibility*, WASH. STATE DEP'T HEALTH.
[19] WASH. REV. CODE § 43.70.545.
[20] *Washington State Public Health Data Exchange Eligibility*, WASH. STATE DEP'T HEALTH.
[21] WASH. REV. CODE § 43.70.057(5).
[22] 2021-23 First Supplemental Budget Session, Policy Level – Q4 – Maintain Core Public Health Systems, WASH. STATE DEP'T HEALTH.
[23] HIV in Washington State, WASH. STATE DEP'T HEALTH.
[24] *Comprehensive Hospital Abstract Reporting System (CHARS)*, WASH. STATE DEP'T HEALTH.
[25] WASH. REV. CODE § 43.70.545.
[26] WASH. REV. CODE § 43.70.545.
[27] *Engrossed Second Substitute House Bill 1272 CHARS Implementation*, WASH. STATE DEP'T HEALTH.
[28] *Community Health Assessment Tool*, WASH. STATE DEP'T HEALTH.
[29] Washington Emergency Medical Services Information System. WASH. STATE DEP'T HEALTH.
[30] Electronic Laboratory Reporting, WASH. STATE DEP'T HEALTH.
[31] Washington Disease Reporting System (WDHRS), WASH. STATE DEP'T HEALTH.
[32] Sexually Transmitted Infections (STIs) Data, WASH. STATE DEP'T HEALTH.
[33] WASH. REV. CODE § 246.101.115.
[34] WASH. REV. CODE § 246.101.115.
[35] WASH. REV. CODE § 246.101.115.
[36] WASH. REV. CODE § 246.101.205.
[37] WASH. REV. CODE §§ 246.101.605, .615.
[38] WASH. REV. CODE § 246.101.615.
[39] WASH. REV. CODE § 246.101.615.
[40] WASH. STATE DEP'T HEALTH, NOTIFIABLE CONDITIONS: HEALTH CARE PROVIDERS/FACILITIES (2023).
[41] *Washington State Local Health Jurisdictions*, WASH. STATE DEP'T HEALTH.
[42] Guthrie S. Birkhead & Christopher M. Maylahn, *State and Local Public Health Surveillance in the United States*, *in* PRINCIPLES & PRACTICE OF PUBLIC HEALTH SURVEILLANCE (3d ed. 2010).
[43] *Disease Reporting Requirements for King County Health Care Professionals*, KING CNTY. PUB. HEALTH.
[44] WASH. ADMIN. CODE § 246-101-505.
[45] WASH. ADMIN. CODE § 246-101-505.
[46] WASH. REV. CODE §§ 43.20.050, 70.28.032, 70.104.055, 43.70.545, 70.24.130.
[47] WASH. ADMIN. CODE § 246-101-605.
[48] WASH. ADMIN. CODE § 246-101-605.
[49] S.B. 6110, 68th Leg., Reg. Sess. (Wash. 2024).
[50] WASH. REV. CODE § 43.70.512.
[51] WASH. REV. CODE § 43.70.550.
[52] WASH. REV. CODE § 43.70.610.

[53] WASH. REV. CODE § 43.70.670.
[54] WASH. REV. CODE § 43.70.770.
[55] WASH. REV. CODE § 43.70.810.
[56] Hazel Glenn Beh, *The Role of Institutional Review Boards in Protecting Human Subjects: Are We Really Ready to Fix a Broken System?*, 26 LAW & PSYCH. REV. 1 (2002).
[57] *Federal Policy for the Protection of Human Subjects ('Common Rule')*, U.S. DEP'T HEALTH & HUM. SERVS., OFF. FOR HUM. RSCH. PROTS.; Protection of Human Subjects, 45 C.F.R. § 46 (2023); *The Belmont Report*, U.S. DEP'T HEALTH & HUM. SERVS., OFF. FOR HUM. RSCH. PROTS.
[58] 45 C.F.R. § 46.101(f).
[59] 45 C.F.R. § 46.102(l).
[60] WASH. ADMIN. CODE § 388-04-070.
[61] U.S. NAT'L INST. HEALTH, CENT. RES. FOR GRANTS & FUNDING INFO., DECISION TOOL: AM I DOING HUMAN SUBJECTS RESEARCH?.
[62] U.S. DEP'T HEALTH & HUM. SERVS., OFF. FOR HUM. RSCH. PROTS., OHRP E-LEARNING PROGRAM, LESSON 2: WHAT IS HUMAN SUBJECTS RESEARCH? 15.
[63] 45 C.F.R. § 46.104.
[64] 45 C.F.R. § 160.103.
[65] 45 C.F.R. § 46.102(e)(7).
[66] WASH. ADMIN. CODE §§ 388-04-030; 388-04-040; HUM. RSCH. REV. SECTION, WASH. DEP'T SOC. & HEALTH SERVS., *Washington State Agency Policy on Protection of Human Research Subjects*, (2020).
[67] WASH. REV. CODE § 42.48.010(4); WASH. ADMIN. CODE § 388-04-020(1).
[68] *Washington A.A.G. Communication, Assessment on Behavioral Risk Factor Surveillance* (June 16, 2011) (on file with author).
[69] 45 C.F.R. § 46.
[70] WASH. REV. CODE §§ 42.48; 42.48.020; WASH. ADMIN. CODE § 388-04-030; *Human Subjects and Public Health Practice: Guidelines for Ethical Data Collection*, WASH. STATE DEP'T HEALTH (Dec. 2008).
[71] *WA DOH Policy 03.001*, WASH. STATE DEP'T HEALTH (Oct. 1, 2017) (on file with author).
[72] WASH. ADMIN. CODE § 388-04-040.
[73] WASH. REV. CODE § 42.48.030.
[74] 45 C.F.R. § 46.109(b)(c).
[75] 45 C.F.R. § 46.116(b).
[76] 45 C.F.R. § 46.116(d).
[77] WASH. REV. CODE § 42.48.020.
[78] WASH. REV. CODE § 70.02.210.
[79] WASH. REV. CODE § 42.48.050.
[80] WASH. STATE DEP'T HEALTH, HUMAN SUBJECTS AND PUBLIC HEALTH PRACTICE: GUIDELINES FOR ETHICAL DATA COLLECTION, 4–5 (Dec. 2008).
[81] WASH. REV. CODE § 42.48.040.
[82] JAMES G. HODGE, JR., *Chapter 8: Public Health Information Management, Privacy & Security*, *in* PUBLIC HEALTH LAW IN A NUTSHELL 293–94 (4th ed. 2022).
[83] James G. Hodge, Jr. & Lawrence O. Gostin**,** *Public Health Practice vs. Research: A Report for Public Health Practitioners Including Cases and Guidance for Making Decisions*, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS ADVISORY COMM. (May 24, 2004).
[84] *Human Subject Regulations Decision Charts: 2018 Requirements*, U.S. DEP'T HEALTH & HUM. SERVS., OFF. FOR HUM. RSCH. PROTS. (June 23, 2020); *Human Subjects and Public Health Practice: Guidelines for Ethical Data Collection*, WASH. STATE DEP'T HEALTH (Dec. 2008); James G. Hodge, Jr. & Lawrence O. Gostin**,** *Public Health Practice vs. Research: A Report for Public Health Practitioners Including Cases and Guidance for Making Decisions*, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS ADVISORY COMM. (May 24, 2004).
[85] *Human Subjects and Public Health Practice: Guidelines for Ethical Data Collection*, WASH. STATE DEP'T HEALTH (Dec. 2008).
[86] James G. Hodge, Jr. & Lawrence O. Gostin, *Revamping the Federal Common Rule: Modernizing Human Participant Research Regulations*, 317 JAMA 1521 (Feb. 22, 2017).
[87] JAMES G. HODGE, JR., *Chapter 8: Public Health Information Management, Privacy & Security*, *in* PUBLIC HEALTH LAW IN A NUTSHELL 261 (4th ed. 2022).

[88] *Health Insurance Portability & Accountability Act of 1996*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 27, 2022).
[89] WASH. REV. CODE § 70.02.005; WASH. CONST. art. I, § 7.
[90] Peninsula Counseling Center v. Rahm, 719 P.2d 926, 935-36 (Wash. 1986) (citing Whalen v. Roe, 429 U.S. 589 (1977)); Alsager v. Bd. of Osteopathic Med. & Surgery, 196 Wash. App. 653 (2016) (citing Murphy v. State, 115 Wash. App. 297 (2003)).
[91] JAMES G. HODGE, JR., *Chapter 8: Public Health Information Management, Privacy & Security*, *in* PUBLIC HEALTH LAW IN A NUTSHELL 261 (4th ed. 2022).
[92] 45 C.F.R. § 160.103.
[93] 45 C.F.R. § 164.514.
[94] *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPPA) Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS.
[95] WASH. REV. CODE § 70.02.010; 45 C.F.R. § 160.103.
[96] State v. Johnson & Johnson, No. 84140-8-I, 2023 Wash. App. LEXIS 1433, at *1 (Wash. Ct. App. July 31, 2023); WASH. ADMIN. CODE § 246-08-390.
[97] Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, § 123 Stat. 226, 246 (2009).
[98] 45 C.F.R. § 164.514.
[99] Matt Moneypenny, *What it Means to be HIPPA Compliant (It's Surprising)*, ETATICS (Sept. 29, 2020).
[100] WASH. REV. CODE § 42.56.250.
[101] WASH. REV. CODE § 70.02.280.
[102] WASH. REV. CODE § 71A.12.360.
[103] WASH. REV. CODE §§ 48.43.0161, 43.371.020.
[104] WASH. REV. CODE § 70.127.295.
[105] WASH. REV. CODE § 43.17.425.
[106] WASH. REV. CODE § 70.320.020.
[107] WASH. ADMIN. CODE § 246-492-020.
[108] WASH. ADMIN. CODE § 246-455-085.
[109] *Department of Health Agency Standards for Reporting Data with Small Numbers*, WASH. STATE DEP'T HEALTH (May 2018).
[110] JAMES G. HODGE, JR., *Chapter 8: Public Health Information Management, Privacy & Security*, *in* PUBLIC HEALTH LAW IN A NUTSHELL 261 (4th ed. 2022).
[111] *Washington State Agency Privacy Principles*, WATECH.
[112] 45 C.F.R. §§ 160.103; 164.500; WASH. ADMIN. CODE § 246-08-390; WASH. REV. CODE §§ 70.02.010(6), (17).
[113] *Syringe Service Programs*, WASH. STATE DEP'T HEALTH; Bob Lutz et al., WASHINGTON STATE NALOXONE DISTRIBUTION PLAN (2022).
[114] 45 C.F.R. § 164.502(b).
[115] 45 C.F.R. § 164.502(b).
[116] WASH. REV. CODE § 70.02.120.
[117] 45 C.F.R. § 164.512(b).
[118] WASH. REV. CODE § 42.56.590.
[119] 45 C.F.R. § 164.508; WASH. REV. CODE §§ 70.02.050(2)(b), 70.02.030.
[120] NAT'L COMM'N TO TRANSFORM PUB. HEALTH DATA SYS., ROBERT WOOD JOHNSON FOUND., Charting a Course for an Equity-Centered Data System (Oct. 1, 2021).
[121] Jane Freemantle, INDIGENOUS CHILDREN – THEIR HUMAN RIGHTS, MORTALITY, AND THE MILLENNIUM DEVELOPMENT GOALS 36 (2010).
[122] Volk v. DeMeerleer, 386 P.3d 254, 258, 270 (Wash. 2016).
[123] WASH. REV. CODE §§ 70.02.350, .050.
[124] 45 C.F.R. §§ 164.500, .104.
[125] 45 C.F.R. §§ 164.502 et seq.
[126] 45 C.F.R. § 164.508.
[127] 45 C.F.R. § 164.510.
[128] 45 C.F.R. § 164.512.
[129] 45 C.F.R. § 164.502; Peninsula Counseling Center v. Rahm, 719 P.2d 926, 935-36 (Wash. 1986).

[130] 45 C.F.R. § 164.514(d)(3)(iii).
[131] 45 C.F.R. § 164.514(e).
[132] 45 C.F.R. § 164.514 (e)(4)(i).
[133] Adapted from *Emergency Preparedness Disclosure*, U.S. DEP'T HEALTH & HUM. SERVS.
[134] S. 631 - Upholding Protections for Health and Online Location Data Privacy Act of 2023, 118th Cong. (2023).
[135] Chris D. Linebaugh et al., *The American Privacy Rights Act*, CONG. RSCH. SERV. LEGAL SIDE BAR 11161 (2024).
[136] WASH. REV. CODE §§ 70.02.005-905.
[137] WASH. REV. CODE §§ 70.02.902, .030.
[138] WASH. REV. CODE §§ 48.43.505, 70.02.045.
[139] WASH. REV. CODE §§ 70.02.050, .220(7).
[140] WASH. REV. CODE § 70.02.005.
[141] WASH. REV. CODE § 70.02.290.
[142] WASH. REV. CODE § 70.02.170.
[143] *Department of Health Policy No. 17.005, Responsibilities for Confidential Information*, WASH. STATE DEP'T HEALTH (Dec. 1, 2017) (on file with author); *Procedures for Policy 17.005 Responsibilities for Confidential Information*, WASH. STATE DEP'T HEALTH (on file with author).
[144] *Department of Health Policy No. 17.006, Release of Confidential Data/Information*, WASH. STATE DEP'T HEALTH (Dec. 1, 2017) (on file with author); *Internal and External Confidential Data Sharing Procedures*, WASH. STATE DEP'T HEALTH (on file with author); JENNIFER BROWN, LEGITIMATE REASONS FOR SHARING DATA (July 12, 2022) (on file with author).
[145] WASH. REV. CODE § 43.105.054; WASH. REV. CODE §§ 39.26.340, .240.
[146] WASH. ADMIN. CODE § 246-08-390(4)(c).
[147] *Protecting Washingtonians' Personal Health Data & Privacy*, WASH. OFF. ATT'Y GEN.; WASH. REV. CODE §§ 19.373.005 et seq.
[148] WASH. REV. CODE § 19.373.010.
[149] WASH. REV. CODE § 19.373.020.
[150] WASH. REV. CODE § 19.373.070.
[151] WASH. REV. CODE § 19.373.030.
[152] WASH. REV. CODE § 19.373.040.
[153] WASH. REV. CODE § 19.373.050.
[154] WASH. REV. CODE §§ 19.373.080, .010.
[155] WASH. REV. CODE § 19.373.090.
[156] WASH. REV. CODE §§ 19.373.010; 19.373.100(1)(a)(i), (1)(a)(ii), (1)(a)(viii) et seq.
[157] Hannah Norman & Victoria Knight, *Should You Worry About Data from Your Period-Tracking App Being Used Against You?*, KFF HEALTH NEWS (May 13, 2022); Eva Epker, *Survey Finds Women's Health Apps Are Among the Least Trusted: What to Know and How to Keep Your Data as Safe as Possible*, FORBES (May 16, 2023); Jon Healey, *Mental Health Apps May put your privacy at risk. Here's what to look for*, L.A. TIMES (May 2, 2023).
[158] Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, 85 Fed. Reg. 25,510 (May 1, 2020) (codified at 42 C.F.R. pts. 406, 407, 422, 423, 431, 438, 457, 482, 485, and 45 C.F.R. pt. 156).
[159] Health Breach Notification Rule, 88 Fed, Reg, 37819 (proposed June 8, 2023) (to be codified at 16 C.F.R. pt. 318).
[160] 42 U.S.C. 2000e (1978).
[161] Elisa Strauss, *Fired for Being Pregnant: Another Kind of Discrimination Women Face at Work*, CNN (Feb. 1, 2018).
[162] Owen Jones, *We Can't Go Back to the Deadly HIV Stigma of the 1980s*, THE GUARDIAN (Nov. 11, 2015).
[163] Benjamin W. Cramer, *A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance,* 8 J. INFO. POL'Y 5, 5–33 (2018).
[164] *The Color of Surveillance*, GEORGETOWN LAW, CTR. ON PRIV. & TECH.
[165] BRENNAN CTR. JUST., SOCIAL MEDIA SURVEILLANCE BY HOMELAND SECURITY INVESTIGATIONS: A THREAT TO IMMIGRANT COMMUNITIES AND FREE EXPRESSION (2019).

[166] NAT'L COMM'N TO TRANSFORM PUB. HEALTH DATA SYS., ROBERT WOOD JOHNSON FOUND., Charting a Course for an Equity-Centered Data System (Oct. 1, 2021).
[167] WASH. REV. CODE §§ 49.60.180, .178, .510, .030; WASH. ADMIN. CODE § 162-16-200; WASH. REV. CODE § 71A.10.040.
[168] *Employment Laws: Disability & Discrimination*, OFF. DISABILITY EMP. POL'Y.
[169] WASH. REV. CODE § 49.60.180.
[170] WASH. REV. CODE § 49.60.178.
[171] WASH. REV. CODE § 5.60.060.
[172] WASH. REV. CODE §§ 49.60, 510; 5.60.060.
[173] WASH. STATE OFF. ATT'Y GEN. BOB FERGUSON, WASHINGTON HEALTH FACILITIES: GUIDANCE & MODEL POLICIES TO ASSIST IN THE IMPLEMENTATION OF THE KEEP WASHINGTON WORKING ACT 13 (2020).
[174] WASH. REV. CODE § 43.17.425.
[175] WASH. STATE OFF. ATT'Y GEN. BOB FERGUSON, WASHINGTON HEALTH FACILITIES: GUIDANCE & MODEL POLICIES TO ASSIST IN THE IMPLEMENTATION OF THE KEEP WASHINGTON WORKING ACT (2020); WASH. REV. CODE §§ 70.170.060, 70.129.005, 70.127.140, 9.02.100, 74.09.875, 74.09.675; WASH. ADMIN. CODE § 388-472-0005.
[176] *Immigrants*, WASH. HEALTH PLAN FINDER.
[177] WASH. REV. CODE § 43.17.425.
[178] JAMES G. HODGE, JR., *Chapter 8: Public Health Information Management, Privacy & Security*, *in* PUBLIC HEALTH LAW IN A NUTSHELL 270-71 (4th ed. 2022).
[179] 45 C.F.R. §§ 160.103, 164.306.
[180] 45 C.F.R. § 164.304.
[181] 45 C.F.R. §§ 164.308, .310.
[182] WASH. ADMIN. CODE § 246-08-390.
[183] *Department of Health Policy No. 17.006, Release of Confidential Data/Information*, WASH. STATE DEP'T HEALTH. (Dec. 1, 2017).
[184] WASH. REV. CODE § 43.105.006; *Agency Overview*, WATECH.
[185] WASH. REV. CODE §§ 43.105.054; 39.26.340, 39.34.240.
[186] *Data Classification Standard*, WATECH (Feb. 11, 2023); DATA SHARING AND IMPLEMENTATION GUIDANCE WATECH (Mar. 2022).
[187] WASH. REV. CODE § 42.56.010.
[188] WASH. REV. CODE § 42.56.080.
[189] Wallin v. Wash. Dep't of Corr., No. 55795-9-II, 2023 WL 5932815, at *1 (Wash. Ct. App. Sept. 12, 2023).
[190] WASH. ADMIN. CODE § 246-08-390.
[191] WATECH, DATA SHARING AND IMPLEMENTATION GUIDANCE (Mar. 2022).
[192] *Policy No. 141: Securing Information Technology Assets*, OFF. CHIEF INFO. OFFICER (Oct. 1, 2011).
[193] *Data Classification Standard*, WATECH (Feb. 11, 2023).
[194] *Encryption Standard*, WATECH (Dec. 11, 2017).
[195] WASH. REV. CODE § 43.105.470.
[196] Matt Dumiak, *NIST Releases AI-focused Privacy Draft Guidance*, COMPLIANCE POINT BLOG (Dec. 22, 2023).
[197] *Interim Guidelines for Purposeful and Responsible Use of Generative Artificial Intelligence*, EA-01-01-G, WATECH, WASH. STATE OFF. CHIEF INFO. OFFICER (OCIO) (Aug. 8, 2023).
[198] *Public Records Act Deskbook: Washington's Public Disclosure and Open Meetings Laws* § 4.2, WASH. STATE BAR ASS'N (Lexis 2020); WASH. ADMIN. CODE § 388-01-090; Planned Parenthood of the Great Nw. v. Bloedow, 350 P.3d 660, 666 (Wash Ct. App. 2015); Seattle Children's Hosp. v. King Cty, 483 P.3d 785, 793, 795-96 (Wash. Ct. App. 2020); WASH. REV. CODE § 43.105.351.
[199] WASH. REV. CODE §§ 70.02.290, 19.215.020; *State Agencies Records Retention Schedules*, WASH. STATE ARCHIVES.
[200] WASH. REV. CODE § 70.02.290.
[201] WASH. STATE OFF. SEC'Y STATE, PUBLIC HEALTH RECORDS RETENTION SCHEDULE VERSION 4.2 (2021).
[202] WASH. OFF. SEC'Y STATE, LOCAL GOVERNMENT COMMON RECORDS RETENTION SCHEDULE (CORE) (2021).
[203] Planned Parenthood of the Great Nw. v. Bloedow, 350 P.3d 660, 666 (Wash Ct. App. 2015).
[204] WASH. REV. CODE § 70.02.050(2)(a).
[205] Seattle Children's Hosp. v. King Cty, 483 P.3d 785, 793, 795-96 (Wash. Ct. App. 2020).

[206] Wash. Pub. Emp's Ass'n v. Wash. State Ctr. for Childhood Deafness & Hearing Loss, 194 Wash. 2d 448, 450 P.3d 601 (2019).
[207] WASH. ADMIN. CODE § 246-08-390.
[208] Securing Information Technology *Assets*, WASH. STATE OFF. CHIEF INFO. OFFICER (Feb. 11, 2023).
[209] WASH. REV. CODE § 39.26.340.
[210] *Data Request FAQ*, WASH. STATE DEP'T HEALTH.
[211] WASH. REV. CODE §§ 39.26.340, 39.34.240.
[212] WASH. REV. CODE § 43.70.020.
[213] WASH. REV. CODE §§ 70.58A.520; WASH. ADMIN. CODE §§ 246-490-020, -030.
[214] WASH. REV. CODE §§ 43.70.665, .050.
[215] WASH. REV. CODE §§ 70.02.230, .260, .265, .310, .340.
[216] WASH. ADMIN. CODE § 246-490-110; Protected Health Care Services—Reproductive Health Care and Gender-Affirming Treatment, HB 1469, 68th Legis., 2023 Reg. Sess. (Wash. 2023); *Reproductive and Gender-Affirming Care: Shielding Providers, Seekers, and Helpers from Out-of-State Legal Actions*, WASH. OFF. OF ATT'Y GEN.
[217] WASH. REV. CODE §§ 70.24.450; 70.02.220, .300; WASH. ADMIN. CODE § 246-101-635.
[218] WASH. REV. CODE § 70.168.090; WASH. ADMIN. CODE § 246-976-420.
[219] WASH. REV. CODE § 70.225.40; WASH. ADMIN. CODE § 246-470-090; 42 C.F.R. pt. 2.
[220] WASH. REV. CODE § 70.58A.520; WASH. ADMIN. CODE § 246-490-030.
[221] WASH. REV. CODE § 70.58A.520.
[222] WASH. REV. CODE § 43.70.052.
[223] WASH. REV. CODE § 70.54.250; *Cancer Surveillance System (CSS)*, FRED HUTCH CANCER CTR.
[224] WASH. REV. CODE § 70.02.230.
[225] WASH. ADMIN. CODE § 246-490-110.
[226] Protected Health Care Services—Reproductive Health Care and Gender-Affirming Treatment, HB 1469, 68th Legis., 2023 Reg. Sess. (Wash. 2023).
[227] WASH. ADMIN. CODE § 246-455-085(7); 42 C.F.R. §§ 2.1 et seq.
[228] SB 5536, 68th Leg., 1st Spec. Sess. (Wash. 2023).
[229] Wash. Dep't of Health Data Matrix (on file with authors).
[230] WASH. REV. CODE §§ 43.70.150, .052, .050, .130, .57; 70.245.150, 70.83.020, 70.54.450, 70.05.170, 70.56.020, 70.168.090.
[231] WASH. REV. CODE § 42.56.100.
[232] WASH. REV. CODE §§ 42.56.625, 42.56.360, 43.70.052, 70.02.050; WASH. ADMIN. CODE § 246-490-110.
[233] WASH. REV. CODE §§ 42.48.020, 70.54.250, 43.70.057.
[234] WASH. REV. CODE §§ 43.70.052, 70.54.450(8); WASH. ADMIN. CODE §§ 246-650-050(4)(b), 246-08-390.
[235] WASH. REV. CODE § 70.225.040(3).
[236] WASH. ADMIN. CODE § 246-490-110; WASH. REV. CODE § 70.245.150.
[237] WASH. REV. CODE § 42.48.020.
[238] WASH. REV. CODE § 70.02.050.
[239] WASH. REV. CODE § 9.02.100.
[240] WASH. ADMIN. CODE § 110-01-0205.
[241] WASH. REV. CODE § 70.02.240(7).
[242] WASH. REV. CODE § 70.02.240(8).
[243] WASH. ADMIN. CODE § 388-01-150.
[244] 8 U.S.C. § 1373.
[245] *Guidance Concerning Immigration Enforcement*, WASH. STATE OFF. ATT'Y GEN. (Apr. 2017).
[246] WASH. REV. CODE § 43.70.595.
[247] WASH. REV. CODE § 70.123.076.
[248] WASH. REV. CODE § 71.24.665.
[249] Letter from Stephen Kutz to WA DOH Secretary Umair Shah (June 16, 2021) (on file with authors).
[250] WASH. REV. CODE § 43.70.052; WASH. ADMIN. CODE § 246-455-020.
[251] WASH. REV. CODE §§ 70.02.230, .250.
[252] WASH. REV. CODE § 72.09.585.
[253] WASH. REV. CODE § 71.24.670.
[254] *Syndromic Surveillance (RHINO)*, WASH. STATE DEP'T HEALTH.

[255] DATA & SURVEILLANCE WORKGROUP, CTRS. FOR DISEASE CONTROL & PREVENTION, DATA AND SURVEILLANCE WORKGROUP REPORT (Nov. 3, 2022).
[256] Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007 (2022); U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104698, TRIBAL EPIDEMIOLOGY CENTERS: HHS ACTIONS NEEDED TO ENHANCE DATA ACCESS (2022).
[257] WASH. REV. CODE § 39.34.240.
[258] WASH. REV. CODE § 43.376.020.
[259] WASH. REV. CODE § 70A.02.010.
[260] *Tribal Public Health*, WASH. STATE DEP'T HEALTH.
[261] WASH. REV. CODE § 70.05.060.
[262] Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007 (2022).
[263] WA DOH Definitions for Data Governance Roles, Eric Kruger, Nov. 19, 2019 (on file with authors).
[264] WA DOH Definitions for Data Governance Roles, Eric Kruger, Nov. 19, 2019 (on file with authors).
[265] WASH. REV. CODE §§ 43.70.057(6)(a)(i)(A), 70.58A.520.
[266] *Data Request FAQ*, WASH. STATE DEP'T HEALTH.
[267] Release of Confidential Data Procedure – DSA (on file with authors).
[268] WASH. REV. CODE § 39.26.010.
[269] WASH. REV. CODE § 39.26.340; *Data Sharing Policy*, SEC-08, WATECH OCIO (Feb. 11, 2023).
[270] WASH. REV. CODE § 43.70.057.
[271] WASH. REV. CODE § 43.70.057.
[272] WATECH, DATA SHARING AND IMPLEMENTATION GUIDANCE (2022).
[273] WASH. REV. CODE § 39.34.240.
[274] WASH. REV. CODE § 39.34.020.
[275] WASH. REV. CODE § 39.34.240.
[276] *Data Classification Standard*, WATECH (Dec. 11, 2017).
[277] *Department of Health Agency Standards for Reporting Data with Small Numbers*, WASH. STATE DEP'T HEALTH (May 2018).
[278] *CHARS Data Sharing Agreement Template*, WASH. STATE DEP'T HEALTH (Sep. 2019).
[279] *Internal and External Confidential Data Sharing Procedures*, WA DOH (on file with authors).
[280] Department of Health External Data Sharing Agreement Template (on file with authors).
[281] WA DOH Flowchart – When a DSA is Required (on file with authors).
[282] WORLD HEALTH ORG., WHO DATA PRINCIPLES (2020).
[283] WASH. REV. CODE § 70.38.015.
[284] WORLD HEALTH ORG., WHO GUIDELINES ON ETHICAL ISSUES IN PUBLIC HEALTH SURVEILLANCE (2017); INT'L ASSOC. NAT'L PUB. HEALTH INSTS., PUBLIC HEALTH SURVEILLANCE: A CALL TO SHARE DATA (2016); Jussi Sane & Michael Edelstein, CHATHAM HOUSE: ROYAL HOUSE GLOB. AFFS., OVERCOMING BARRIERS TO DATA SHARING IN PUBLIC HEALTH: A GLOBAL PERSPECTIVE (2015); Pinky Langat et al., *Is There a Duty to Share? Ethics of Sharing Research Data in the Context of Public Health Emergencies*, 4 PUB. HEALTH EMERGENCIES 4 (2011); Lisa Lee et al., *Ethical Justification for Conducting Public Health Surveillance Without Patient Consent*, 102 AM. J. PUBLIC HEALTH 38 (2012).
[285] James G. Hodge, Jr., Torrey Kaufman & Craig Jaques, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS, LEGAL ISSUES CONCERNING IDENTIFIABLE HEALTH DATA EXCHANGES BETWEEN STATE PUBLIC HEALTH AUTHORITIES AND TRIBAL EPIDEMIOLOGY CENTERS IN SELECT U.S. JURISDICTIONS (2011).
[286] 410 Ill. Comp. Stat. 501/10(a) (2023); Stephen Murphy, *Improving Local Public Health Access to Public Health Data: Illinois Out Front*, NETWORK FOR PUB. HEALTH L. (Jan. 19, 2024).
[287] James G. Hodge, Jr., Torrey Kaufman & Craig Jaques, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS, LEGAL ISSUES CONCERNING IDENTIFIABLE HEALTH DATA EXCHANGES BETWEEN STATE PUBLIC HEALTH AUTHORITIES AND TRIBAL EPIDEMIOLOGY CENTERS IN SELECT U.S. JURISDICTIONS (2011).
[288] James G. Hodge, Jr. & Lawrence O. Gostin, *Public Health Practice vs. Research: A Report for Public Health Practitioners Including Cases and Guidance for Making Decisions*, COUNCIL OF STATE & TERRITORIAL EPIDEMIOLOGISTS ADVISORY COMM. (May 24, 2004).
[289] MODEL STATE EMERGENCY HEALTH POWERS ACT § 1-103(9).
[290] 410 Ill. Comp. Stat. 501/5 (2023).
[291] WASH. REV. CODE § 70.38.025.
[292] Lawrence O. Gostin, James G. Hodge, Jr. & Ronald O. Valdiserri, *Informational Privacy and the Public's Health: The Model State Public Health Privacy Act*, AM. J. PUB. HEALTH 1388, 1389 (2001).

[293] Alicia Martinz-Garcia et al., *FAIR Principles to Improve the Impact on Health Research Management Outcomes*, 5 HELIYON e15733 (2023).
[294] *Pseudonymization*, NAT'L INST. OF STANDARDS & TECH (visited on Feb. 26, 2024).
[295] Lawrence O. Gostin, James G. Hodge Jr., & Ronald O. Valdiserri, *Informational Privacy and the Public's Health: The Model State Public Health Privacy Act*, AM. J. PUB. HEALTH 1388, 1391 (2001).
[296] Willem G. van Panhuis et al., *A Systematic Review of Barriers to Data Sharing in Public Health*, 14 BMC PUB. HEALTH 1144 (2014).
[297] WASH. REV. CODE §§ 70.02.005-905.
[298] WASH. REV. CODE § 70.02.020.
[299] WASH. REV. CODE §§ 70.02.030, .040.
[300] WASH. REV. CODE § 70.02.050.
[301] WASH. REV. CODE §§ 70.02.200, .220.
[302] WASH. REV. CODE § 70.02.220.
[303] WASH. REV. CODE §§ 70.02.230, .240.
[304] WASH. REV. CODE § 70.02.010.
[305] WASH. REV. CODE § 70.02.280(1).
[306] CHATHAM HOUSE: ROYAL HOUSE GLOB. AFFS., A Guide to Sharing the Data and Benefits of Public Health Surveillance (2017).
[307] WASH. REV. CODE § 70.58A.520.
[308] WASH. REV. CODE § 43.70.052(9)(a)(ii).
[309] WASH. REV. CODE § 43.70.052(9)(a)(i).
[310] 410 Ill. Comp. Stat. 501/15 (2023).
[311] WASH. REV. CODE § 39.34.240.
[312] WA DOH Definitions for Data Governance Roles, Eric Kruger, Nov. 19, 2019 (on file with authors).
[313] WA DOH Definitions for Data Governance Roles, Eric Kruger, Nov. 19, 2019 (on file with authors).
[314] GLOB. RSCH. COLLAB. FOR INFECTIOUS DISEASE PREPAREDNESS, PRINCIPLES OF DATA SHARING IN PUBLIC HEALTH EMERGENCIES (2018).
[315] WASH. REV. CODE § 43.70.057.
[316] 410 Ill. Comp. Stat. 501/10(a) (2023).
[317] *Suppression of Rates and Counts*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 8, 2023).
[318] *Public-Use Data Files*, CTRS. FOR DISEASE CONTROL & PREVENTION (Feb. 24, 2022).
[319] *Data User Agreement*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 11, 2020).
[320] *Pseudonymization*, NAT'L INST. OF STANDARDS & TECH (visited on Feb. 26, 2024).