

# The Sedona Conference WG11 Brainstorming Group Outline – Impact of Pandemic Response on Global Privacy (October 2021)



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **The Sedona Conference WG11 Brainstorming Group Outline – Impact of Pandemic Response on Global Privacy (October 2021)**

### **Brainstorming Group Members:**

Mark Bailey (Brainstorming Group Leader)  
Natalie Gonzalez  
Ron Hedges  
Carrie Parikh  
David Sella-Villa  
Caren Shiozaki  
Mihran Yenikomshian  
Jonathan Wilan (Steering Committee Liaison)

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

Outline: Impact of Pandemic Response on Global Privacy  
(Working Draft for discussion at WG11 Houston midyear meeting)

**Introduction**

We have been asked to explore the conflict that exists between the tools used to control pandemics and the risks that these tools pose to privacy interests. Because we conclude that this could be a promising topic for a Commentary, we propose the following preliminary ideas and recommendations on a potential Commentary.

Our research revealed 1) the scope and variety of the strategies and tools that are available to combat pandemics (which we are currently calling “Pandemic Mitigation Tools”); and 2) the complex patchwork of federal and state privacy laws that are potentially implicated by the Pandemic Mitigation Tools. We believe the best way to attack this problem is to identify and describe the Pandemic Mitigation Tools that have the clearest privacy nexus and evaluate each of them through the lens of the applicable laws.

We recognize that public health officials frequently deploy Pandemic Mitigation Tools in combination with one another. This greatly enhances the Tools’ utility, while also multiplying the risks they pose to privacy interests. We also recognize that governments may partner with private companies to deploy the tools. The paper will address these two related complicating factors.

In the course of our research and writing, we will evaluate whether the current legal framework adequately balances society’s interest in containing pandemics with individuals’ interest in privacy. If our analysis reveals that any Pandemic Mitigation Tool is governed by a thorough and coherent legal framework, we will explain that framework for the benefit of practitioners and judges. If our analysis reveals major gaps or flaws in the legal framework surrounding any Pandemic Mitigation Tool, we may supplement the analysis with suggested legislative or regulatory improvements.

The proposed paper begins with a high-level review of the legal background and then describes the state and federal laws that relate to pandemics and privacy. Next, the paper identifies and explains the Privacy Mitigation Tools that might impact privacy rights. The paper then evaluates the legal framework that applies to each of the Pandemic Mitigation Tools. If, as we research and write, we see gaps in the law or areas that need improvement, we will consider the best approach to make suggestions for legislators and regulators.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

In response to a few of the questions posed by the Steering Committee:

1. **Geographic Scope.** We recommend focusing our analysis on state and federal laws in the United States. Having surveyed the applicable legal authorities, we believe it will be challenging enough to address these issues within the framework of American law. If the analysis expands to foreign laws, we are not confident that we could develop a Commentary that would be useful to practitioners. Of course, to the extent foreign laws are part of the legal framework – *e.g.*, a company that might participate in public/private partnerships might be governed by GDPR – they may need to be addressed.
2. **Will the Commentary provide helpful guidance for the future?** It is not yet clear whether the COVID-19 pandemic reflects a point-in-time challenge and if so, whether the analysis can be expanded or abstracted so as to make it useful to future practitioners. At first blush, there appears to be a need for this Commentary. When a pandemic or other emergency occurs, courts and practitioners are called upon to decide complex issues, often very quickly, at a time when society is under extreme stress. So it behooves us to think carefully about these questions before they arise. Further, there appear to be parallels with other emergent issues, including the advances in technology that will change the way “routine” health care and public health services are delivered. Moreover, pandemics and similar events may become increasingly more common, as humanity continues to encroach on natural environments, climate change makes certain locations more hospitable to viruses and bacteria, bioterrorism remains a threat, and humans continue to handle and manipulate dangerous pathogens in the laboratory setting.
3. **Are there specific legal principles to apply?** It appears that the analysis can be grounded in specific legal principles and frameworks. Even if these principles and frameworks are not fully developed for application to pandemics, the skeleton is there in the form of statutes, regulations, and judicial opinions that address confidentiality, data security, privacy, and the balance between individual rights and the government’s role in protecting its citizens.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## Legal background

### I. Legal Foundations of Emergency Response

#### A. Sources of State Authority

1. After the people, the states are the source of political power in the United States. This broad power is referred to as the “police power.” Accordingly, a state can enact legislation or take any action that would not otherwise violate that state’s law or the U.S. Constitution. This could include compliance with applicable federal laws because of the supremacy principles.
2. “According to settled principles, the police power of a state must be held to embrace, at least, such reasonable regulations established directly by legislative enactment as will protect the public health and the public safety.” *Jacobson v. Commonwealth of Massachusetts*, 197 U.S. 11, 25 (1905) (internal citations omitted). In the *Jacobson* case Massachusetts enacted a law that allowed cities to enforce vaccination of citizens. The U.S. Supreme Court held such a law constitutional because it was consistent with the state’s police power.

#### B. Sources of Federal Authority

1. The U.S. Constitution enumerates the powers of the Federal government. Though the Federal government has primary jurisdiction over matters of national security and foreign affairs, States have primary authority for addressing emergent situations that arise in other contexts. Natural disasters and pandemics are emergent situations for which the Federal government lacks primary jurisdiction.
2. Federal emergency response programs, though, can help address emergent situations through Federal spending authority. A state’s receipt of Federal funds can be conditioned on the state’s compliance with a wide variety of requirements. Those requirements may include data privacy protections. **Potential research:** Compile and categorize a representative list of such federal laws.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## II. Federal Laws

### A. Americans with Disabilities Act of 1990 (ADA) & Rehabilitation Act

1. Americans with Disabilities Act (ADA)
  - a. [42 U.S.C. §§ 12101 et seq](#) [42 U.S.C. § 12112\(d\) Discrimination](#)
  - b. Rehabilitation Act (Rehab Act)
  - c. [29 U.S.C. §§ 701 et seq \(Chapter 16 Vocational Rehabilitation and Other Rehabilitation Services\)](#)
2. Overview: The [ADA](#) prohibits discrimination and guarantees that people with disabilities have the same opportunities as everyone else to participate in the mainstream of American life — to enjoy employment opportunities, to purchase goods and services, and to participate in State and local government programs and services. Modeled after the Civil Rights Act of 1964, which prohibits discrimination on the basis of race, color, religion, sex, or national origin – and Section 504 of the Rehabilitation Act of 1973 — the ADA is an “equal opportunity” law for people with disabilities.
3. The ADA, at [42 U.S.C. § 12112\(d\)](#), generally prohibits medical examinations and inquiries of job applicants unless the inquiry is about the ability of the applicant to perform job related functions. The ADA **does** authorize medical examinations and inquiries by employers with regard to an employee’s request for reasonable accommodation for a disability. In both instances, there are confidentiality requirements that attach to the records and information gathered.
4. The [Rehabilitation Act of 1973](#) (also known as the “Rehab Act”) prohibits discrimination on the basis of disability in programs run by federal agencies; programs that receive federal financial assistance; in federal employment; and in the employment practices of federal contractors. The standards for deciding if employment discrimination exists under the Rehab Act are the same as those used in Title I of the ADA.
5. *NOTE: The ADA has restrictions on when and how much medical information an employer may obtain from any applicant or employee. Prior to making a conditional job offer to an applicant,*

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

*disability-related inquiries and medical exams are generally prohibited. They are permitted between the time of the offer and when the applicant begins work, provided they are required for everyone in the same job category. Once an employee begins work, any disability-related inquiries or medical exams must be job related and consistent with business necessity. See CDC guidance, including the CDC's "[Interim Public Health Recommendations for Fully Vaccinated People](#)." The EEOC monitors CDC publications.*

- a. *employers to keep confidential any medical information they learn about any applicant or employee. Medical information includes not only a diagnosis or treatments, but also the fact that an individual has requested or is receiving a reasonable accommodation (reasonable accommodation may include religious exemptions to vaccine requirements)*
  - i <https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>

## **B. Clinical Laboratory Improvement Amendments of 1988 (CLIA)**

1. [42 U.S.C. § 263a](#)
2. Overview
  - a. In general terms, the CLIA regulations establish quality standards for laboratory testing performed on specimens from humans, such as blood, body fluid and tissue, for the purpose of diagnosis, prevention, or treatment of disease, or assessment of health. The Centers for Medicare & Medicaid Services (CMS) regulates all laboratory testing (except research) performed on humans in the U.S. through CLIA. In total, CLIA covers approximately 254,000 laboratory entities. The Division of Laboratory Services, within the Survey and Certification Group, under the Center for Clinical Standards and Quality (CCSQ) has the responsibility for implementing the CLIA Program.
  - b. Disclosure of Results: CLIA regulations allow laboratories to give a patient, or a person designated by the patient, his or her “personal representative,” access to the patient’s completed test reports on the patient’s or patient’s personal representative’s request. To align with this requirement, the

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule also provides individuals (or their personal representatives) with the right to access test reports directly from laboratories subject to HIPAA (CLIA-certified or CLIA-exempt laboratories). While patients can also get access to their laboratory test reports from their doctors, they have the option to obtain their test reports directly from the laboratory while maintaining strong protections for patients' privacy. The rules are issued jointly by three agencies within the U.S. Department of Health and Human Services: the Centers for Medicare & Medicaid Services (CMS), which is generally responsible for laboratory regulation under CLIA, the Centers for Disease Control and Prevention (CDC), which provides scientific and technical advice to CMS related to CLIA, and the Office for Civil Rights (OCR), which is responsible for enforcing the HIPAA Privacy Rule.

### **C. E-Government Act of 2002 (Section 208)**

1. [44 U.S.C. § 3501 note](#) See also, [Public Law 107-347](#)
  - a. **Overview:** Privacy Impact Assessments (“PIAs”) are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form. A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. The Act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns, reveal classified (i.e., national security) information, or sensitive (e.g., potentially damaging to a nation interest, law enforcement effort or competitive business interest contained in the assessment) information.

### **D. Federal Information Security Modernization Act of 2014 (FISMA)**

1. [44 U.S.C. Chapter 35 \(44 U.S.C. §§ 3551-3558\)](#)



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. Overview: The Federal Information Security Modernization Act requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.
  - a. The Federal Information Security Modernization Act of 2014 (FISMA) was codified in the E-Government Act of 2002 as the Federal Information Security Management Act of 2002 (44 U.S.C. § 3501 note), and was reauthorized in 2014 (Pub. L. 113-283). The statute pertains to information security, which is defined as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and c) availability, which means ensuring timely and reliable access to and use of information.”  
Source: [44 U.S.C. § 3552\(b\)\(3\)](#)

## **E. Federal Records Act of 1950 (FRA)**

1. [44 U.S.C. Chapter 31 et seq](#)
2. Overview: The FRA provides that “the head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency’s activities.” [[44 U.S.C. § 3101](#)]
  - a. The implementation of the FRA is overseen by the Archivist of the United States, who heads the National Archives and Records Administration (NARA). The Archivist provides “guidance and assistance to Federal agencies with respect to ensuring adequate and proper documentation of the policies and transactions of the Federal Government and ensuring proper records disposition.” [[44 U.S.C. § 2904](#)]

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **F. Family Educational Rights and Privacy Act (FERPA)**

### **1. [20 U.S.C. § 1232g](#)**

- a. Overview:** FERPA protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.
- b.** FERPA permits educational agencies and institutions, such as Local Education Agencies (LEA) and their constituent schools, to disclose PII from education records to State Education Agencies (SEA) and other State educational authorities without a parent's prior consent under certain conditions. For a review of the exceptions to the general prior consent rule in FERPA, see 34 CFR § 99.31.
- c. Health or Safety Emergency Exception:** FERPA prohibits educational agencies (e.g., school districts) and institutions (i.e., schools) from disclosing PII from students' education record without the prior written consent of a parent or "eligible student," unless an exception to FERPA's general consent rule applies. 20 U.S.C. §§ 1232g(b)(1) and (b)(2); 34 C.F.R. §§ 99.30 and 99.31. For instance, pursuant to one such exception, the "health or safety emergency" exception, educational agencies and institutions may disclose to a public health agency PII from student education records, without prior written consent in connection with an emergency if the public health agency's knowledge of the information is necessary to protect the health or safety of students or other individuals. 20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. §§ 99.31(a)(10) and 99.36.
  - i. [FERPA & Coronavirus Disease 2019 \(COVID-19\) Frequently Asked Questions](#)**

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **G. Federal Policy for the Protection of Human Subjects (Common Rule)**

1. [42 U.S.C. § 289](#)
2. Overview: The Federal Policy for the Protection of Human Subjects or the “Common Rule” was published in 1991 and codified in separate regulations by 15 Federal departments and agencies. The HHS regulations, 45 CFR part 46, include four subparts: subpart A, also known as the Federal Policy or the “Common Rule”; subpart B, additional protections for pregnant women, human fetuses, and neonates; subpart C, additional protections for prisoners; and subpart D, additional protections for children. A fifth subpart, subpart E, which concerns registration of Institutional Review Boards (IRBs) was added in 2009. For all participating departments and agencies, the Common Rule outlines the basic provisions for IRBs, informed consent, and Assurances of Compliance. Human subject research conducted or supported by each Federal department/agency is governed by the regulations of that department/agency. The head of that department/agency retains final judgment as to whether a particular activity it conducts or supports is covered by the Common Rule. If an institution seeks guidance on implementation of the Common Rule and other applicable Federal regulations, the institution should contact the department/agency conducting or supporting the research.
  - a. Office of Human Research Protections (OHRP) Guidance on Coronavirus: <https://www.hhs.gov/ohrp/regulations-and-policy/guidance/ohrp-guidance-on-covid-19/index.html>

## **H. Genetic Information Nondiscrimination Act of 2008 (GINA)**

1. [42 U.S.C. § 1320d-9, Application of HIPAA Regulations to Genetic Information](#) [42 U.S.C. § 12112\(d\)\(3\), Employment Entrance Examination](#) *See also:* [Public Law 110-233](#)
2. Overview: The Genetic Information Nondiscrimination Act (GINA) protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

3. Title I of GINA includes provisions that generally prohibit group health plans and health insurance issuers from discriminating based on genetic information. These provisions amend the Employee Retirement Income Security Act (ERISA), administered by the Department of Labor; the Public Health Service Act (PHS Act), administered by the Department of Health and Human Services (HHS); and the Internal Revenue Code (the Code), administered by the Department of Treasury (the Treasury) and the Internal Revenue Service (IRS). The Department of Labor has jurisdiction with respect to employment-based group health plans. HHS in conjunction with the States administers these provisions with respect to health insurance issuers. The Treasury and IRS administer these provisions with respect to employers. Title I of GINA also includes individual insurance market provisions under the PHS Act and privacy and confidentiality provisions under the Social Security Act, which are both within the jurisdiction of HHS.
4. Title II of GINA prohibits the use of genetic information in making employment decisions in any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoffs, training, fringe benefits, or any other term or condition of employment. It is enforced by the Equal Employment Opportunity Commission (EEOC).
  - a. **Note:** The Genetic Information Nondiscrimination Act (GINA) prohibits employers from asking employees medical questions about family members. GINA, however, does not prohibit an employer from asking employees whether they have had contact with anyone diagnosed with COVID-19 or who may have symptoms associated with the disease. Moreover, from a public health perspective, only asking an employee about his contact with family members would unnecessarily limit the information obtained about an employee's potential exposure to COVID-19.  
<https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>

## **I. Health Insurance Portability and Accountability Act of 1996 (HIPAA Breach Notification Rule)**

1. [42 U.S.C. § 17932](#) See also: [Health Information Technology for Economic and Clinical Health \(HITECH\) Act \(Public Law 111-5, Div. A, title XIII, § 13402\)](#) See also: [45 C.F.R. §§ 164.400-414 \(Subpart D\)](#)

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

2. **Overview:** Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (the “Act”) requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of the U.S. Department of Health and Human Services (HHS) following the discovery of a breach of unsecured protected health information. In some cases, the Act requires covered entities also to provide notification to the media of breaches. In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach. Finally, the Act requires the Secretary to post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.
  - a. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

#### **J. Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy Rule)**

1. [Health Insurance Portability and Accountability Act of 1996 \(Public Law 104-191\)45 C.F.R. Part 160 45 C.F.R. Part 164 Subparts A and E](#)
2. **Overview:** The HIPAA Privacy Rule, adopted by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

#### **K. Health Insurance Portability and Accountability Act of 1996 (HIPAA Security Rule)**

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

1. [\*\*Health Insurance Portability and Accountability Act of 1996 \(Public Law 104-191\)\*\*](#)*See also: [45 C.F.R. Part 160](#)*  
*See also: [45 C.F.R. §§ 164.102-106 and §§ 164.302-318](#)*

2. **Overview:** The HIPAA Security Rule, adopted by the U.S. Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act of 1996 establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

**L. NOTE HIPAA and COVID-19:** The HHS Office for Civil Rights (OCR) has provided Bulletins, Notifications of Enforcement Discretion, Guidance, and Resources that help explain how patient health information may be used and disclosed in response to the COVID-19 nationwide public health emergency.

1. These documents discuss both the HIPAA Privacy and Security Rules including guidance on flexibilities and guidance on disclosure, and enforcement discretion.
  - a. [HIPAA and COVID-19 | HHS.gov](#)
  - b. **Note:** The Secretary of the Department of Health and Human Services (HHS) may waive or modify certain Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requirements after determining that: a) a disease or disorder presents a public health emergency (PHE); or b) that a public health emergency, including significant outbreaks of infectious disease or bioterrorist attacks, otherwise exists under **section 319 of the Public Health Service (PHS) Act**.

**M. Paperwork Reduction Act of 1995 (PRA)**

1. [44 U.S.C. Chapter 35 et seq](#)
2. **Overview:** The Paperwork Reduction Act (PRA), signed into law in 1980 and reauthorized in 1995, provides the statutory framework for the Federal government's collection, use, and dissemination of information. The goals of the PRA include (1) minimizing



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

paperwork and reporting burdens on the American public and (2) ensuring the maximum possible utility from the information that is collected.

- a. In support of these goals, the PRA requires Federal agencies to take specific steps before requiring or requesting information from the public. These steps include (1) seeking public comment on proposed information collections and (2) submitting proposed collections for review and approval by the Office of Management and Budget (OMB). Within OMB, the Office of Information and Regulatory Affairs (OIRA) carries out the information collection review.
- b. One of the purposes of the Paperwork Reduction Act is to “ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to (A) privacy and confidentiality, including section 552a of title 5; (B) security of information, including section 11332 of title 40; and (C) access to information, including section 552 of title 5.” 44 U.S.C. § 3501(8).
- c. **Note:** Section 319(f), recently added by the 21st Century Cures Act, allows the HHS Secretary to determine that the circumstances of a Public Health Emergency(PHE) or a disease or disorder, including a novel and emerging public health threat that is significantly likely to become a PHE, **necessitate a waiver from PRA requirements**. If the Secretary makes such a determination, then PRA requirements for voluntary collection of information do not apply during the immediate investigation of and response to the PHE during the period of the PHE or the time period necessary to determine if a disease or disorder, including a novel and emerging public health threat, will become a PHE.

## N. Privacy Act of 1974 (Privacy Act)

1. [5 U.S.C. § 552a](#)
2. **Overview:** The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires U.S. Government agencies give public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.

#### **O. Public Health Service Act (Certificates of Confidentiality)**

1. [42 U.S.C. Ch. 6A 42 U.S.C. § 241\(d\) Protection of privacy of individuals who are research subjects](#)
2. **Overview:** Under section 301(d) of the Public Health Service Act (42 U.S.C. § 241(d)), the Secretary of the U.S. Department of Health and Human Services may authorize persons engaged in biomedical, behavioral, clinical, or other research to protect the privacy of individuals who are the subjects of that research. This authority has been delegated to the National Institutes of Health (NIH). Persons authorized by the NIH to protect the privacy of research subjects may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify them by name or other identifying characteristic.

#### **P. Public Health Service Act (Confidentiality of Health Statistics)**

1. [42 U.S.C. Ch. 6A](#) *See also:* [42 U.S.C. § 242m\(d\)](#)  
*See also:* [Section 308\(d\) of the Public Health Service Act](#)
2. **Overview:** The Public Health Service Act, 42 U.S.C. Ch. 6A, provision regarding the confidentiality of health statistics prohibits the National Center for Health Statistics (NCHS) from using any personal information for any purpose other than what was described to survey participants and from sharing that information with anyone not clearly mentioned to them. This provision enables NCHS to assure respondents strict confidentiality.



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

### III. State Laws

- A. Some states have laws requiring government agencies to dispose of personal identifying information (“PII”) when it is no longer needed, implement reasonable policies to protect PII, and provide notice of certain data breaches. *See, e.g.*, C.R.S. §§ 24-73-101–103. PII often includes health and biometric information. *Id.*

#### B. Emergency Powers Acts

1. Most if not all States have Emergency Powers Acts.
2. These Acts sometimes contain limitations on the State’s power to infringe upon individual rights, including the right to privacy.
  - a. For example, in enacting South Carolina’s “Emergency Health Powers Act,” the legislature found that “the rights of people to liberty, bodily integrity, and privacy must be respected to the fullest extent possible consistent with the overriding importance of the public’s health and security.” S.C. Code Ann. § 44-4-110(9).
  - b. Some legislatures have considered bills that expressly recognize privacy limitations in government emergency response. *See, e.g.*, H.B. 20B-1013 (introduced in Colorado legislature but not enacted) (“emergency orders . . . issued by state or local officials that bind, curtail, or infringe the rights of private parties must be narrowly tailored to serve a compelling public health or safety purpose”).
  - c. **Potential Research:** We will likely conduct a 50-state survey of emergency response statutes to identify and analyze any data privacy requirements.
3. Some state public health laws governing pandemic response contain express privacy protections. For example, under Colorado law, “reports and records resulting from the investigation of epidemic and communicable diseases . . . shall be strictly confidential” and may only be released under narrowly defined circumstances. *See* C.R.S. § 25-1-122(4).
4. Executive orders issued by governors under emergency authority frequently contain limiting language relating to individual rights,

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

including privacy and confidentiality. *See, e.g.,* [Colorado Public Health Order 20-27](#) (requiring hospitals to submit data about COVID-19 patients and medical resource availability, and requiring that “Any patient identifiable information collected will be held as confidential and will not be shared publicly.”

5. Many states have laws requiring companies to dispose of personal identifying information (“PII”) when it is no longer needed, protect information, and provide notice of certain data breaches. *See, e.g.,* C.R.S. §§ 6-1-713, 6-1-713.5, 716.

#### **IV. Constitutional Limitations**

- A. Collection of certain kinds of information (*i.e.*, geolocation data) could implicate the 4<sup>th</sup> and 1<sup>st</sup> Amendments of the U.S. Constitution. *See United States v. Antoine Jones*, 132 S.Ct. 945 (2012) (placement of a GPS tracking device to a vehicle to monitor the vehicle’s movements was covered by the Fourth Amendment.

### **Analysis**

#### **V. Overview of key tools and strategies used to protect public health during a pandemic**

##### **A. CONTACT TRACING**

##### **1. What it is**

- a. This is a public health practice utilized by health departments to identify and notify people who have been exposed to someone with an infectious disease.
- b. To mitigate SARS-CoV-2 (the virus that causes COVID-19), health departments deploy contact tracing and the subsequent quarantine of exposed contacts in an attempt to limit the number of infected contacts who propagate viral transmission.
- c. The goal of COVID-related contact tracing is to identify people that were in close contact (within six feet) with infected individuals for 15 minutes or more, two days prior to symptom onset or two days prior to a positive test if the person is asymptomatic.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **2. Manual approach to contact tracing**

- a. Contact Tracers will reach out to people who have tested positive for COVID-19 infections. This may be in person or via phone call, text or eMail. The infected parties will be asked who they may have exposed while they were contagious.
- b. That group of people will be contacted to inform them of their potential exposure to the virus. Contact Tracers and the health department for which they work will keep confidential the name of the person who tested positive and exposed them.

## **3. Digital contact tracing**

- a. As the pandemic progressed, health departments recognized that contact tracing and related case management supported by digital tools could enhance overall program functionality.
- b. Additionally, many companies are looking at technology based solutions to manage COVID-related processes as they build plans to bring employees back into the office.
- c. Digital tools include:

## **4. Proximity tracking**

- a. Proximity tracking technology measures the signal strength between two interconnected devices. As applied to COVID mitigation, proximity data generated by mobile devices are analyzed to determine whether they were close enough for a long-enough duration for there to have been virus transmission. If an individual is infected, those within a pre-defined proximity of the infected individual will be notified. Appropriate next steps to reduce health risks are then given to the suspected individual.
- b. In some industries (e.g., construction) contact tracing efforts are automated and digitized by issuing wearables to workers. The workers' interactions and duration of contact are collected and analyzed in real time. The wearable device will issue an alert if two workers violate proximity and duration parameters. All of the data collected is stored for management reporting.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **5. Case management**

- a. Person-to-person outreach for potential exposure notifications can be very slow if done the manual way. Digital contact tracing systems involve “virtual agents” that automatically handle outreach via phone calls or text messages.

## **6. Contact tracing data management**

- a. As organizations begin executing their re-opening plans, many are collecting COVID-related information on their employees. Most companies are not familiar with the stringent data privacy and protection requirements under HIPAA. As they become aware, information governance and data management programs either need to be developed or revised.

# **VI. TESTING**

## **A. Types of tests**

1. Molecular: This type of test detects the RNA (i.e., nucleic acid) component of the virus. The most commonly used form is the PCR (polymerase chain reaction) test. This is frequently performed by testing a nasal swab specimen. Molecular tests need to be processed by a laboratory, with results available within 24 hours.
2. Antigen: This test detects the proteins from the virus. The advantage of this test is that it can return results in as little as 15 minutes, don't require a laboratory to process results, and are cheaper to produce. They detect the virus in people who are still highly infectious, and therefore are useful for isolation and quarantine purposes. The downside is that these tests are not as sensitive as molecular tests so more likely to return false negative results. Many of the at-home kits are for antigen tests.
3. Antibody: This type of testing looks for antibodies that were created to combat the virus. This test will only identify if the individual had the virus in the past.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **B. Who receives the test results?**

1. Testing Entities: Testing may be performed by various entities:
  - Self (using the at-home kits)
  - Medical entities (e.g., personal physician or a medical group)
  - Government agency (e.g., Department of Health)
  - Third party (e.g., Walgreens et. al. health services companies)
2. Disposition of test results: State laws generally require that vaccine providers keep records on paper or in an electronic database. State boards of health are usually the overseers of the records.
3. Medical entities: Medical entities and government agencies do store the test results. There may be inter and intra entity data sharing. Anonymization of patient identities depends on the circumstances and requirements for sharing.
4. Corporations: Some corporations are contracting with third parties to provide testing to their employees. Under those contracts, the employer is provided the test results of the employees that use those services.
5. At-Home Testing: Providers of at-home test kits are considered third party service providers. Some of the at-home kits provide results within the confines of the user's home. Other tests allow for the collection of the sample by the user in their home but require the collection to be sent to a laboratory for processing (e.g., Vault). Other at-home tests require the use of a mobile application that connects to a digital analyzer for results to be processed and reported in real time (e.g., the Ellume test kit).

The extent of data stored for an individual using third party services will vary. The individual must ascertain what is being collected by viewing the privacy policies. For example, CVS maintains the details (including results) of testing. According to the Ellume privacy policy, they capture location and device information, but they do not store the test results.

Third party providers will do data sharing with other third parties. Again, the extent of sharing will vary and will be outlined in their privacy policy.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

## **VII. EVIDENCE OF IMMUNITY**

### **A. Proof of vaccination**

1. (For the US) When an individual receives their COVID vaccination, they are issued a CDC card. This will show
  - Name
  - Date of vaccinations (1<sup>st</sup> and 2<sup>nd</sup> if applicable)
  - Where the vaccination was administered
  - Which vaccine was administered
  - Vaccine lot (batch) number

### **B. Vaccine Passport**

1. COVID-19 vaccine passports are applications (smartphone or online) that show a person has been vaccinated. At this time, the US government is not issuing vaccine passports, and has no plans to do so. See next section.

### **C. Digital vaccination records**

1. A number of organizations are working on digital alternatives to the paper-based CDC card. These are applications that allow the uploading, storing and viewing of vaccination documents on a smartphone. Some examples:
  - a. The *Vaccine Credential Initiative* is a coalition of public ii. and private organizations seeking to make vaccination records more accessible online.
  - b. *IBM Health Pass* is a platform on which users can collect health documents and data into a “digital wallet” on their smartphones. IBM also partnered with Salesforce on a project to develop ways that can help organizations and businesses verify the health status of employees and customers.
  - c. Some states have created their own applications – for example, New York issues the *Excelsior Pass* to show vaccination or negative test results.

## **VIII. INFORMATION SHARING**

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- A. A number of data repositories have been established to support global scientific research related to COVID-19. E.g., IHME state-by-state projections; Johns Hopkins global interactive map, Open ICPSR GitHub and other free “research” tools.
- B. Healthcare providers, payers and healthcare clearinghouses providing info to public health officials.
- C. Healthcare providers, payers and healthcare clearinghouses who serve self-funded plans being asked to share COVID related information for non-healthcare related purposes like return to work and workers compensation claims.
- D. Organizations required to report details of employees who test positive to public health officials. Organizations permitted to share limited COVID data to other employees for workplace protection purposes as outline in OSHA.
- E. Public health providing data to municipalities (e.g., state of Maine – received information on people who tested positive for COVID so that first responders could be prepared when responding to emergency calls)
- F. [Kittery asks state to share addresses of coronavirus patients - Portland Press Herald](#)
- G. Data sharing for AI purposes. Detection and Prevention. AI can be harnessed for forecasting the spread of virus and developing early warning systems by extracting information from social media platforms, calls and news sites and provide useful information about the vulnerable regions and for prediction of morbidity and mortality. Bluedot identified a cluster of pneumonia cases and predicted the outbreak and geographical location of the COVID-19 outbreak based on available data using machine learning. HealthMap collects the publicly available data on COVID-19 and makes it readily available to facilitate the effective tracking of its spread. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7692869/>
- H. AI can augment mobile health applications where smart devices like watches, mobile phones, cameras and range of wearable device can be employed for diagnosis, contact tracing and efficient monitoring in COVID-19. Applications like AI4COVID-19 that rely on audio recording samples of 2 s cough can be used in telemedicine.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

- I. AI in Monitoring, early diagnosis, reducing the burden from medical practitioners & healthcare staff
- J. Data sharing with unusual suspects: concert venues, travel and hospitality, Broadway, sport teams, etc. What is their obligation to keep your vaccine status safe when you offer it voluntarily to attend an event?

## **IX. Pandemic Mitigation Tools are usually used in combination**

- A. Pandemic Mitigation Tools do not work in isolation from one another. The true benefit of these tools is amplified when they are working in concert.
  - 1. Contact tracing is complemented by widespread, rapid, and accessible testing so exposed individuals can quickly be tested and isolate.
  - 2. Further, mobile phone applications have great potential to benefit the public as it can assist with contact tracing by identifying individuals who are unknown to the infected individual, recording/communicating testing results, and vaccine verification. If this information was combined with medical information, there could be opportunities to help prioritize outreach to high-risk exposed patients leading to better health outcomes and more efficient delivery of care when healthcare systems are stretched thin.
  - 3. However, to gain more benefit from these Pandemic Mitigation Tools, information needs to be shared across different groups potentially reducing individual privacy. It is important to take into consideration the tradeoffs between giving up some privacy for public benefit.
- B. The tradeoffs between benefits and privacy may change when taking a holistic view of these tools used together. Considerations for tradeoffs include:
  - 1. Goal Prioritization
    - a. A goal of Pandemic Mitigation Tools is to stop/slow the spread of a disease but also to help avoid economic shutdowns and to keep services like schools open. Pandemic



This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

Mitigation Tools may be deployed to avoid large-scale shuttering of the economy.

## 2. Population of focus

- a. The benefits of these tools may be different depending on the population they are deployed in such as the general public or specific groups of individuals (e.g., companies, schools)
- b. Universities have integrated many of these Pandemic Mitigation Tools together (e.g., testing or no access to buildings, using Wi-Fi to identify close contacts) and can control movement in and out of their own networks better than the general population.
- c. The general public has a much larger and more diverse population (e.g., children, elderly, jobs that can be done remotely commuters, poor access to testing and knowledge of technology).

## 3. Opting-in or Opting-out

- a. Tools where users “opt-in” have lower privacy concerns as notifications disclose the privacy implications. The trade-off is that there are typically fewer people using Pandemic Mitigation Tools when people have to opt-into them vs opt-out of them.

## 4. Data/Information sharing

- a. Today, it is nearly impossible for one organization (whether public or private) to deploy all the Pandemic Mitigation Tools. Partnerships and information sharing between organization is vital to enhance the effectiveness of these tools.
- C. Further, the benefits of such Pandemic Mitigation Tools may depend on how widespread disease is spreading in a community (e.g., the value of contact tracing and testing is higher when there are low positivity rates in a community and low spread).
- D. Since using Pandemic Mitigation Tools will likely require coordination and information sharing with various organizations, these tools should strive for transparency in the following:

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

1. Who is getting the data and how is it used?
2. What are the potential benefits to the individual?
3. What are the potential benefits to the community when information is shared?
4. How is the information stored and for how long?

## **X. Public/Private partnerships**

- A. Joint action between public and private entities might be subject to laws governing both private and public actors.
  1. In other words, a state actor cannot use a private company to evade constitutional and statutory limitations on state conduct.
  2. And if government agencies work with private businesses, they may subject themselves to the requirements of state privacy laws, *e.g.*, the California Consumer Privacy Act / California Privacy Rights Act.
    - a. As a matter of policy, there should be strict limitations on use and strong confidentiality provisions to ensure that private interests do not improperly monetize the data they are provided.

## **XI. Analysis of privacy laws governing the pandemic mitigation tools**

- A. For each Pandemic Mitigation Tool, we intend to address the following:
  1. Describe the current legal framework (including statutes, regulations, and case law) governing the use of the Pandemic Mitigation Tool – what is permissible, and where are the limits.
  2. Are there privacy concerns that are not addressed in the current legal framework?
    - a. This includes an analysis of the use of the tools in combination with one another and in the context of public/private partnerships.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org) no later than November 29, 2021.

3. Does the current legal framework create undue obstacles to the successful deployment of the Pandemic Mitigation Tool?

- a. This includes an analysis of the use of the tools in combination with one another and in the context of public/private partnerships.
- B. If there are significant gaps or shortcomings in the law governing any of the Pandemic Mitigation Tools – including risks to privacy and obstacles to public health efforts – we will consider suggesting legislative fixes.
- C. What steps should be taken to mitigate privacy risks in the context of public-private partnerships in the implementation of Pandemic Mitigation Tools.

## **XII. Conclusion**