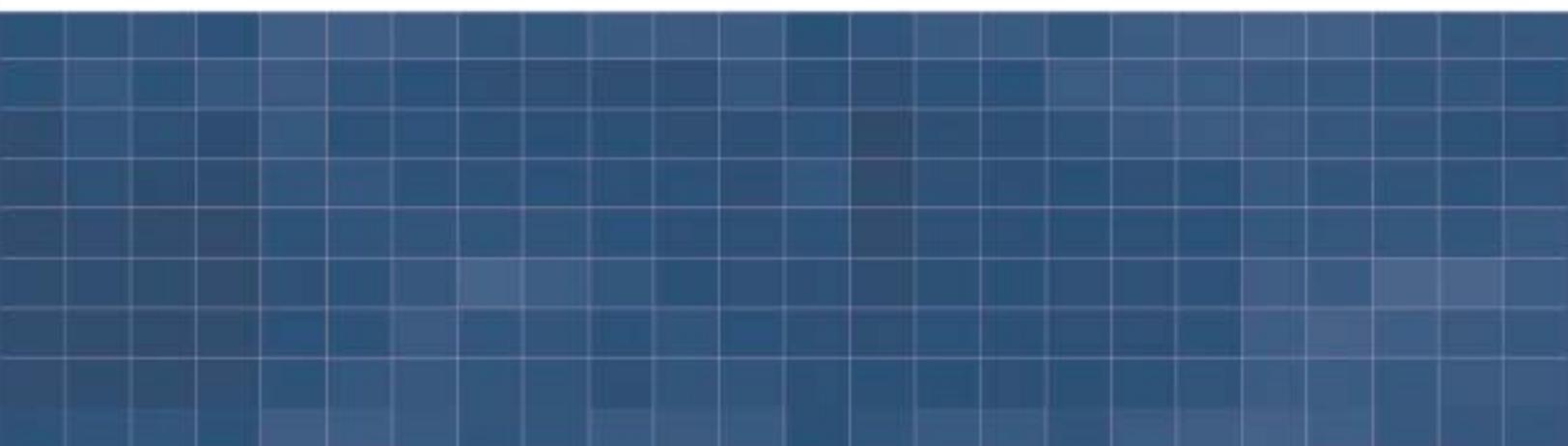




sixty-five  
**65**  
years



## Privacy & Pandemic Flu Guide



This report is supported by funding from the Centers for Disease Control and Prevention Cooperative Agreement to Improve the National's Public Health Infrastructure with State Public Health Agencies/ Systems (#U50/CCU313903-07) ASTHO is grateful for this support.

The report was researched and prepared for the Association of State and Territorial Health Officials by Sterling Elliott, MPH.

For additional information contact: [publications@astho.org](mailto:publications@astho.org)

The Association of State and Territorial Health Officials (ASTHO) is the national nonprofit organization representing the state and territorial public health agencies of the United States, the U.S. Territories, and the District of Columbia. ASTHO's members, the chief health officials of these jurisdictions, are dedicated to formulating and influencing sound public health policy, and to assuring excellence in state-based public health practice.

# Privacy and Pandemic Flu Guide

## Table of Contents

- Executive Summary..... 1
- Background ..... 1
- Introduction..... 1
- Definitions..... 1
  - Scenario 1: Working with non-traditional partners & an Alternate Care Site (ACS)..... 2
  - Scenario 2: Operation of a Working Quarantine..... 3
- Step I: Review of existing laws ..... 4
  - Scenario 1: Review of Existing Legal Framework ..... 6
  - Scenario 2: Review of Existing Legal Framework ..... 7
- Step II: Public Health Activity Checklist ..... 9
  - Scenario 1: Public Health Activity Checklist..... 10
  - Scenario 2: Public Health Activity Checklist..... 11
- Step III: Analysis and Conclusions ..... 13
  - Scenario 1: Analysis and Conclusions..... 13
  - Scenario 2: Analysis and Conclusions..... 13
- Step IV: Solutions ..... 14
  - Scenario 1: Solutions..... 14
  - Scenario 2: Solutions..... 14
- Acknowledgements ..... 15

## Executive Summary

The Privacy and Pandemic Flu Guide is designed to aid public health professionals when privacy concerns are raised about activities related to pandemic flu planning and response. The guide describes four steps that will walk a public health professional through an analysis of the activities. The guide was developed as a result of a May 2007 discussion among a small group of experts in privacy and preparedness. This guide is intended to be a dynamic document, and it is hoped that feedback from the field on its utility will inform future iterations.

## Background

In recent years, much attention has been given to public health legal preparedness, including emergency powers and quarantine and isolation implementation. Public health legal preparedness also involves awareness of federal and state laws that relate to the collection, protection, use, and disclosure of information during public health emergency planning and response. In May 2007, ASTHO convened a group of subject matter experts to discuss privacy issues related to pandemic flu preparedness and response. The group was made of representatives from ten public health jurisdictions, as well as the private sector, national organizations, and federal agencies. This guide is a product of that discussion. It is designed to support public health professionals in protecting the public's health while balancing the need to protect information from wrongful or harmful disclosure.

## Introduction

The Privacy and Pandemic Flu Guide is intended to describe public health response activities in the context of information privacy. The Guide is divided into four steps:

- A review of existing laws
- A public health activity checklist
- Analysis and conclusions
- Solutions

If public health practitioners and lawyers follow all four steps, they should be able to:

- Determine how activities implicate state and federal privacy laws
- Fashion solutions for activities that do not conform to those laws
- Identify laws that might need amending

This guide does not suggest that all activities related to pandemic flu planning and response require a detailed analysis of information pathways, information points, and privacy points. Rather it proposes that when such an analysis is required, i.e., when privacy concerns are raised about an activity, that the evaluator has steps to reach solid conclusions and solutions.

## Definitions

### Activity

A public health response that is part of a pandemic influenza plan, such as operating an alternate care site or a working quarantine.

### Data protection

The storage, transmission, and disposal of data.

### Influenza pandemic

A worldwide epidemic caused by the emergence of a new or novel influenza strain to which humans have little or no immunity and which develops the ability to infect and be transmitted efficiently for a sustained period of time in the community between humans.<sup>1</sup>

### Information pathway or pathway

The path that a piece of information follows through collection, protection, use, and disclosure. Activities might create more than one pathway.

### Information point or point

A specific spot along an information pathway where a public health agency collects, protects, uses, or discloses a piece of information.

### Isolation

Although definitions may vary from state to state, isolation is generally defined as separation or restriction of movement of persons ill with an infectious disease in order to prevent transmission to others.<sup>2</sup>

### Law

Federal and state constitutions, cases, statutes, regulations, administrative codes, and legal opinions.

### Quarantine

Although definitions may vary from state to state, quarantine is generally defined as a restraint upon the activities or communication (e.g., physical separation or restriction of movement within the community/work setting) of an individual(s) who has been exposed to an infection but is not yet ill to prevent the spread of disease; quarantine may be applied voluntarily (preferred) or on a compulsory basis dependent on legal authority.<sup>3</sup>

### Privacy point

An information point that implicates state or federal privacy laws.

### Social distancing

Measures to increase the space between people and decrease the frequency of contact among people.<sup>4</sup>

The following two scenarios will be used to illustrate the application of the guide to pandemic flu response activities.

### **Scenario 1: Working with non-traditional partners & an Alternate Care Site (ACS)**

#### **Background**

- The President has declared a state of emergency for the entire country.
- The Secretary of the US Department of Health and Human Services (HHS) has declared a public health emergency.
- The Governor has declared a state of emergency and a public health emergency and has ordered all public and private primary and secondary schools closed.
- State and local emergency operations centers have been activated to the extent called for under emergency operations and pandemic plans.
- The primary ACS location was recently damaged by fire to the extent that it is unusable for ACS operations. The only other facility is an area high school.

At the ACS, the follow activities occur:

- Patients with flu-like symptoms are triaged depending on the severity of their symptoms.
- Patients that need further care are routed to appropriate facilities.
- First aid is provided.
- Medical supplies, such as anti-viral medication, are provided.
- Patients without transportation are provided transport to their homes or other health care facilities.

A public health preparedness staff person calls the privacy officer and describes the situation:

“It’s the second day of operations at the relocated ACS. Leaders of a local faith-based organization have offered to deliver care to homes and transport patients to the ACS. They have provided us with a list of congregation members and would like the ACS to cross-reference existing records to identify congregation members who have sought triage care. The faith-based organization also wants the ACS staff to ask about religious affiliations when processing new patients, and to provide it with names of individuals who identify its faith on a daily basis.

We want to work with this organization, but are we allowed to collect and disclose this information?

Can we:

- Ask incoming patients about their religious affiliations?
- Give the organization a list of members’ names that have sought and/or are seeking triage care?”

#### **Information Pathways & Points**

**Information pathways in this scenario include:**

1. Intake
2. Patient Referral
3. Disclosure of Patient Identity & Medical Information

**Information points in this scenario include:**

##### **1. Intake**

- Intake of symptoms and medical history at ACS
- Intake of religious affiliation at ACS
- Intake of transportation needs, if any, at ASC
- Symptoms and medical history used to provide first aid, as required
- Information on transportation needs used to inform transportation services offered

##### **2. Patient Referral**

- Patients referred to outside health care providers
- Patient medical history disclosed to outside health care providers

##### **3. Disclosure of Patient Identity & Medical Information**

- Patients’ symptoms and medical histories disclosed to faith-based organization for delivery of health care services in ACS and patient homes

## **Scenario 2: Operation of a Working Quarantine<sup>1</sup>**

### **Background**

- The President has declared a state of emergency for the entire country.
- The Secretary of HHS has declared a public health emergency.
- The Governor has declared a state of emergency and a public health emergency, as applicable.
- State and local emergency operations centers have been activated to the extent called for under emergency operations and pandemic plans.
- The state public health agency's continuity of operations plans has been activated.

As part of the state public health agency's continuity of operations plans, a "working quarantine" has been instituted at locations where public health agency emergency operations center and field staff report to work. This working quarantine includes:

- Collection of baseline health status information at beginning of working quarantine;
- Conducting entrance and exit interviews to determine exposure while working shift and while away from the job;
- Collecting symptom information at beginning and end of shift;
- Documenting and storing information collected.

Public health nurses and doctors that are employees of the state public health agency are staffing the working quarantine stations.

A public health nurse in charge of one working quarantine station calls the public health legal counsel and describes the situation:

"An epidemiologist working in the early stages of the outbreak becomes symptomatic. Information is collected about his symptoms at the beginning of his shift. His supervisor calls the public health nurse and wants to know the epidemiologist's health status and whether to "send him home" if he poses a risk to others.

Further, his co-workers are talking to the supervisor and calling the public health nurse. They want to know the epidemiologist's health status to determine whether they have been put at risk by close contact.

Finally, a local reporter calls and wants to know how many public health employees are sick."

She asks the counsel, "Can I:

- Tell the supervisor that the epidemiologist should not be working for at least 7 days?
- Tell the supervisor or the co-workers that his symptoms showed up today and his earlier interviews and baseline report showed no symptoms?
- Tell the local press that, so far, 9 public health employees have been recorded as symptomatic?"

<sup>1</sup> The definition of working quarantine is "persons are permitted to work but must observe activity restrictions while off duty. Monitoring for fever and other symptoms before reporting for work is usually required. Use of appropriate Personal Protective Equipment while at work is required." Appendix D1: Interventions for Community Containment, Supplement D: Community Containment Measures, Including Non-Hospital Isolation and Quarantine, Public Health Guidance for Community Level Preparedness and Response to Severe Acute Respiratory Syndrome Version 2. Available at: <http://www.cdc.gov/ncidod/sars/guidance/D/app1.htm>.

## Step I: Review of existing laws

Analysis of pandemic flu activities in light of privacy concerns begins with a review of the existing legal framework. This specifically concerns federal and state laws related to the collection, protection, use, and disclosure of health information in emergencies and non-emergencies.

The review should include laws that pertain to the role of the public health agency as:

- a public health authority
- an employer
- a health care provider

Laws might be collected in hard copy or electronic form. Alternately, electronic links to laws should be organized in an accessible manner.

Expertise in specific subjects might lay in distinct areas of the public health agency or in other government agencies. For example, the agency human resource department may already have collected, catalogued, and organized laws related to the employer's role in collecting, protecting, using, and disclosing employee health information. It is important to identify which efforts have already been made (e.g., legal review of state laws related to the exchange of health information as part of the Health Information Privacy and Security Collaboration) and what resources are already available (e.g., state pandemic flu bench books). In many states, the Attorney General's office is also a key partner.

## State Review

### Suggested State Laws

- Laws governing the practice of licensed professionals
- Laws governing the licensing of health facilities
- Mental health laws
- Substance abuse laws
- Health information privacy laws
- Physician-patient records acts
- Freedom of information laws
- Emergency laws
- State occupational health and safety laws

### Suggested Key Word Searching

Language governing the sharing of health information related to pandemic flu activities is frequently scattered among state laws. A key word search in electronic archives is recommended to identify all pertinent laws. Below is a table of suggested key words.

## Key Words

alcohol treatment information	genetic information	private/privacy
avian flu	health information	public health powers
bird flu	identity theft	quarantine
communicable disease	influenza	records retention
confidential/confidentiality	medical examination	rule-making authority
delegation authority	medical records	school closure
disaster	mental health information	security
disclosure	occupational health	social distancing
encryption	open records	special education
emergency	pandemic	substance abuse treatment
freedom of information	personal identification	sunshine law

## **Federal Review**

The following is a list of federal laws suggested for review because they may be implicated in the information pathways and points created by pandemic flu planning and response activities. Some of these laws are focused on privacy issues. Others have an unrelated main focus but do refer, in some way, to the collection, use, protection and/or disclosure of information. These laws relate also to different roles that the public health agency might serve: public health authority, employer, and health care provider.

### **Public Health Authority**

#### ***Family Educational Rights and Privacy Act of 1974 (FERPA)***

FERPA protects the privacy of student education records. Information that is part of the student record, including health information, cannot be disclosed without parental consent or student consent if over the age of 18.

#### ***Freedom of Information Act (FOIA)***

FOIA requires federal agencies to disclose records requested in writing by any person, unless there is a specific exemption

#### ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)***

The HIPAA Privacy Rule establishes regulations for the use and disclosure of protected health information.

#### ***Pandemic and All-Hazards Preparedness Act (PAHPA)***

PAHPA is designed to improve preparedness efforts by centralizing federal responsibilities, requiring state-based accountability, proposing new national surveillance methods, addressing surge capacity, and facilitating the development of vaccines and other scarce resources.

#### ***Privacy Act of 1974***

The Privacy Act of 1974 mandates that administrative and physical security systems be put in place to prevent the unauthorized disclosure of personal records.

#### ***Public Health Services Act (PHSA)***

The PHSA provides legislative authority for research and for programs to prevent and control communicable diseases. It also regulates water purification, sewage treatment systems, pollution of lakes and streams, and biological products; establishes the National Vaccine Program; and provides authority for the issuance of confidentiality certificates and assurances for sensitive data.

## **Health Care Provider**

### ***42 CFR Part 2***

These regulations generally require patient permission prior to disclosure of information about any person who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program, except in emergency situations.

### ***45 CFR Part 46 Common Rule also known as the Federal Policy for the Protection of Human Subjects***

This rule sets up protections for the use of human subjects in research projects. It also lays out policies for institutional review boards that oversee research.

### ***Emergency Medical Treatment and Active Labor Act (EMTALA)***

The EMTALA says that hospitals that both accept Medicare and advertise emergency room services are statutorily required to provide appropriate screening examinations. These examinations determine whether emergency medical conditions exist, regardless of patients' ability to pay.

### ***Clinical Laboratory Improvement Amendments (CLIA)***

CLIA are regulatory standards that apply to all clinical laboratory testing performed on humans in the United States. CLIA includes standards about the parties who may receive laboratory results.

## **Employer**

### ***Americans with Disabilities Act (ADA)***

The ADA prohibits discrimination, under certain circumstances, based on disability. Confidentiality provisions protect employee and applicant medical information. Exceptions permit specified disclosures.

### ***Family and Medical Leave Act of 1993 (FMLA)***

The FMLA ensures that workers of covered employers are able to take extended leaves of absence from work to handle family issues or illness without fear of being terminated from their jobs by their employers or being forced into a lower job upon their return.

## **Another document worth review is:**

### ***Ethical Guidelines in Pandemic Influenza, CDC***

This document is a set of recommendations from the Ethics Subcommittee of the Advisory Committee to the Director, Centers for Disease Control and Prevention.

## **Scenario 1: Review of Existing Legal Framework**

For this situation, the evaluator from State A determines that the federal law most applicable is HIPAA.

### **1. Intake**

Some relevant sections of HIPAA related to information points in Information Pathway #1 (Intake) are:

- 45 CFR Section 164.520(a), which requires notice of a covered entity's privacy practices be given to a patient.
- 45 CFR Section 164.530(j)(1) and Section 164.520(e), which require a written receipt from the patient for the covered entity's Notice of Privacy Practices.
- 45 CFR Section 160.203(c), which provides an exception from HIPAA jurisdiction if a state law confidentiality provision for intervention exists.

The evaluator determines that, in this case, the exception referred to in 45 CFR Section 160.203(c) could be Section 100 of State A Statutes. These say that the Local Emergency Management Director is owner of records for persons with special needs. However, point of distribution triage described in Scenario 1 is for the entire population. Thus, one or more of the somewhat conflicting state laws relevant to Information Pathway #2 Patient Referral will apply. In any event, HIPAA is without jurisdiction in State A, as a state confidentiality law is available for this public health intervention.

An additional HIPAA section relevant to the staff person's concern about collecting religious affiliation is:

- 45 CFR Section 164.510(a)(1)(i)(D), which allows a covered entity to collect a patient's religious affiliation, providing the patient does not object, and use the information for a facility directory. The individual must be given an opportunity to object and must not object before they may be listed in a facility directory.

The evaluator also knows that in at least one past emergency (e.g., Hurricane Katrina), the Secretary of HHS has suspended HIPAA penalties for making directories without authorization.

### **2. Patient Referral**

A relevant section of HIPAA related to information points in Information Pathway #2 (Patient Referral) is:

- 45 CFR Section 164.506(c)(1 and 2), which allows disclosure to other covered entities for treatment purposes without authorization, and minimum necessary record culling is not required when disclosure is for treatment purposes, [45 CFR Section 164.502(b)(2)(i)].

The evaluator determines that public health intervention deference to state law exists in this situation, but considers the different state laws that might apply:

- Section 101 of State A Statutes, related to State Department of Health possessed individual personal health information, does not allow disclosure to other health care providers without written authorization from the patient.
- Section 102 of State A Statutes, related to licensed health care providers' patient records, permits disclosure to other health care providers for care and treatment.
- Section 103 of State A Statutes, related to licensed health care facility patient records, allows disclosure to licensed facility personnel and attending physicians for treatment purposes. However, Rule 001 of State A Administrative Code clarifies disclosure to health care providers not on staff is prohibited even if the disclosure is for treatment.
- Section 104 of State A Statutes requires patient consent to send patient information to a health care provider outside the facility.

The evaluator determines that HIPAA and state practitioner law allow disclosure for treatment; however, state Department of Health law and hospital law require patient authorization.

### **3. Disclosure of Patient Identity & Medical Information**

The evaluator identifies a relevant section of HIPAA to the information points in Information Pathway #3 (Disclosure of Patient Identity & Medical Information):

- 45 CFR Section 164.510 does not limit disclosure of facility directories providing the patient has not objected to inclusion.

Under normal circumstances, the local faith-based organization volunteers could be made non-paid employees and provided basic training on HIPAA privacy rule requirements. Volunteers could then join the ACS workforce as health care workers. In addition, an emergency declaration from the President or Secretary of HHS can suspend the HIPAA requirements for training to allow immediate volunteer utilization. The evaluator notes that in State A, according to the state law addressing confidentiality, the Governor would also have to suspend conflicting state laws. However, State A has a history of gubernatorial suspension of health care licensure requirements to allow other state health care providers to donate services during catastrophic events.

## Scenario 2: Review of Existing Legal Framework

The evaluator reviews State B's laws related to monitoring employee health. These include:

- State B Code 100-200

A covered entity may not require a medical examination and may not make inquiries of an employee as to whether the employee is an individual with a disability or as to the nature or severity of the disability, unless the examination or inquiry is shown to be job-related and consistent with business necessity.

Information obtained regarding the medical condition or history of the applicant is collected and maintained on separate forms and in separate medical files and is treated as a confidential medical record
- State B Code 200-300, Recording criteria

(A) Basic requirement. Each employer required by this part to keep records of fatalities, injuries, and illnesses must record each fatality, injury and illness that:

  - (1) Is work-related; and
  - (2) Is a new case; and
  - (3) Meets one or more of the general recording criteria of 200-300 or the application to specific cases of 200-301 through 200-305.

The evaluator reviews State B's information privacy laws, which include:

- State B Code 100-200

A covered entity may require a medical examination shown to be job-related and consistent with business necessity, but information obtained must be collected and maintained on separate forms and in separate medical files and is treated as a confidential medical record

But supervisors and managers may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations.
- State B Code 400-500

It shall, through its representatives, investigate the causes, character, and means of preventing the epidemic and endemic diseases as the State is liable to suffer from and the influence of climate, location, and occupations, habits, drainage, scavenging, water supply, heating, and ventilation. ... *Patient-identifying information elicited from these records and registries must be kept confidential by the department and it is exempt from the provisions of Chapter 4 of Title 30.*
- State B Code 400-500

(A) Access to protected health information of persons who have participated in medical testing, treatment, vaccination, isolation, or quarantine programs or efforts by the State Department of Health during a public health emergency is limited to those persons having a legitimate need to:

  - (1) *provide treatment to the individual who is the subject of the health information;*
  - (2) conduct epidemiological research; or
  - (3) investigate the causes of transmission.

(B) *Protected health information held by the State Department of Health must not be disclosed to others without individual specific informed authorization except for disclosures made:*

  - (1) directly to the individual;
  - (2) to the individual's immediate family members or life partners;
  - (3) to appropriate state or federal agencies or authorities when necessary to protect the public's health;
  - (4) to health care personnel where needed to protect the health or life of the individual who is the subject of the information;
  - (5) pursuant to a court order or executive order of the Governor to avert a clear danger to an individual or the public's health; or
  - (6) to coroners, medical examiners, or funeral directors or others dealing with human remains to identify a deceased individual or determine the manner or cause of death.

- State B Code 500-600

“Protected health information” means any information, whether oral, written, electronic, visual, pictorial, physical, or any other form, that relates to an individual’s past, present, or future physical or mental health status, condition, treatment, service, products purchased, or provision of care, and that reveals the identity of the individual whose health care is the subject of the information, or where there is a reasonable basis to believe such information could be utilized (either alone or with other information that is, or reasonably should be known to be, available to predictable recipients of such information) to reveal the identity of that individual.

- State B Code 600-700

Records such as ... medical records ... and other records which by law are required to be closed to the public are not considered to be made open to the public under the provisions of this act.

The evaluator determines that two federal laws apply in the case of Scenario 2, the Americans with Disabilities Act (ADA) and HIPAA. Specific sections that are relevant include:

- ADA Regulation 29 CFR 1630.14(c)

Examination of employees. *A covered entity may require a medical examination (and/or inquiry) of an employee that is job-related and consistent with business necessity. A covered entity may make inquiries into the ability of an employee to perform job-related functions.*

*(1) Information obtained under paragraph (c) of this section regarding the medical condition or history of any employee shall be collected and maintained on separate forms and in separate medical files and be treated as a confidential medical record, except that:*

- *(i) Supervisors and managers may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations.*

- HIPAA, 45 CFR 160.103, Definitions

Covered entity means: (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Health information means any information, whether oral or recorded in any form or medium, that: is created or received by a[n] ... employer ... and relates to the past, present, or future physical or mental health or condition of an individual ... .

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and is created or received by a[n] ... employer ... and relates to the past, present, or future physical or mental health or condition of an individual ... and (i) That identifies the individual; or (ii) With respect to which there is reasonable basis to believe the information can be used to identify the individual.

- HIPAA, 45 CFR 160.501, Definitions

Protected health information excludes individually identifiable health information in: ... (iii) *Employment records held by a covered entity in its role as employer.*

## Step II: Public Health Activity Checklist

This checklist supports the analysis of pandemic flu preparedness and response activities in the legal environment for sharing information. For example, it demonstrates what public health staff are doing and what information pathways are utilized so that federal and state laws will attach to specific information points. To be useful to the practitioner, checklists need to be based on specific public health activities. Special attention must be given to the details of collection, protection, use, and disclosure.

### Checklist

#### Data Collection

- Who is collecting the data?  
  
Public health agency employees or representatives?  
  
Employees or representatives of non-public health agency entities?
- What is the role of the entity collecting the data?  
  
Health care provider?  
  
Public health authority?  
  
Employer?  
  
Other?
- What data are being collected?
- In what form are the data being collected?
- From whom are the data being collected?
- What is the purpose of collecting the data?

#### Data Protection

- Storage  
Who stores the data?  
In what form are the data stored?  
How are the data protected?  
How long are the data being retained?
- Transmission  
In what form are the data transmitted?  
How are the data protected?
- Disposal  
How are the data destroyed?  
When are the data destroyed?  
Who destroys the data?

#### Data Use

- What are the data used for?

#### Data Disclosure

- Who is requesting the data?
- If different from the requestor, to whom will the data be disclosed?
- What is the role of the entity or individual requesting the data?
- What specific information is being requested?
- For what purpose are they requesting the data?

### **Scenario 1: Public Health Activity Checklist**

The evaluator uses the checklist to analyze the specific information points that have raised concerns with the staff person. Using the checklist, the privacy officer follows up with the ACS staff person and determines that the ACS is being operated by the State Department of Health as a public health authority. It is intervening to protect the public's health by providing prophylaxis and other measures as needed.

#### **Data Collection**

Who is collecting the data?	Public health agency employees staffing ACS
What is the role of the entity collecting the data?	Public health authority
What data are being collected?	Medical history, religious affiliation
In what form are the data being collected?	Forms completed by hand and later entered into database
From whom are the data being collected?	Patients presenting in the ACS
What is the purpose of collecting the data?	Treatment, referral

#### **Data Protection: Storage, Transmission and Disposal**

Though not specifically pertinent to the ACS staff person's concerns, the privacy officer follows-up on the data storage, transmission, and disposal protocols at the ACS to make sure that there are plans in place to minimize the risk of wrongful or harmful disclosure.

Who stores the data?	ACS
In what form are the data stored?	Access database
How are the data protected while stored?	Hard copy in locked file cabinet, shredded once entered into database, encryption of database, role-based access to database, privacy training of ACS staff and volunteers
How long is the data being retained?	Until ACS is dismantled
In what form are the data transmitted?	Oral and written form
How are the data protected while transmitted?	Privacy training of ACS staff and volunteers
How are the data destroyed?	Paper forms shredded, database deleted
When are the data destroyed?	At least 1 week after ACS is dismantled
Who destroys the data?	ACS staff

### **Scenario 2: Public Health Activity Checklist**

The evaluator uses the checklist to analyze the specific information points that have raised concerns in the staff person.

#### **Data Collection**

Who is collecting the data?	Public health agency employees
What is the role of the entity collecting the data?	Employer
What data are being collected?	Health information
In what form are the data being collected?	Numerical health information, recorded on paper records, anecdotal responses about possible disease exposures
From whom are the data being collected?	Public health agency employees
What is the purpose of collecting the data?	Tracking employee health status during influenza pandemic for three reasons:  Early intervention and treatment  Protects workforce from ill co-worker  Protects public from ill employee

#### **Data Protection: Storage, Transmission, and Disposal**

Though not specifically pertinent to the staff person's concerns, the privacy officer follows-up on the data storage, transmission, and disposal protocols to make sure that there are plans in place to minimize the risk of wrongful or harmful disclosure.

Who stores the data?	Employee health personnel
In what form are the data stored?	Employee health database
How are the data protected while stored?	Entered into database, encryption of database, role-based access to database, privacy training of personnel
How long is the data being retained?	Until employees are terminated
In what form are the data transmitted?	Written form
How are the data protected while transmitted?	Privacy training of personnel
How are the data destroyed?	Not destroyed after working quarantine ends, data become part of employee's permanent health record
When are the data destroyed?	Six months after employees' termination
Who destroys the data?	Employee health personnel

## Data Use

What are the data used for?

Compliance with state occupational health and safety requirements regarding reporting of work-related injuries and illnesses to make decisions about:

- Employee health interventions and treatment
- Removal of employees from field workforce

## Data Disclosure

Who is requesting the data?

Co-workers, supervisor, media

What is the role of the entity requesting the data?

Co-workers, supervisor, media

What specific information is being requested?

Supervisor

- Epidemiologist's health status
- If he poses a risk to others
- 7 day restriction

Co-workers

- Epidemiologist's health status
- When he started showing symptoms

Media

- How many public health employees are sick with pandemic flu

For what purpose are they requesting the data?

Supervisor

- To determine if there is a risk that any co-workers have been exposed
- To make a decision about removing employee from field workforce

Co-worker

- Not specified, but probably to determine if there is a risk that they have been exposed

Media

- To write a news story

## Step III: Analysis and Conclusions

After answering the checklist, the evaluator will consult the collection of laws and documents reviewed in Step I. Using the checklist in Step II, the evaluator will identify information and privacy points on the information pathway created by the activity. An example of a privacy point along a pathway is the collection of communicable disease information from a health care provider.

Once the privacy points have been identified, the evaluator will be able to reach conclusions and determine if there are gaps in the activities or laws that should be modified. Three potential conclusions may result from the analysis:

- Privacy points along the information pathways conform to state and federal privacy laws.
- Some privacy points along the information pathways conform to state and federal privacy laws, and some do not.
- No privacy points along the information pathways conform to state and federal privacy laws.

### **Scenario 1: Analysis and Conclusions**

The evaluator uses the results from Step I and Step II to reach conclusions. It was determined that the ACS is the public health authority performing an intervention. Therefore, it is outside HIPAA jurisdiction. State confidentiality laws; however, do apply. The data collected at information points in Information Pathways #1 (Intake) and #2 (Patient Referral) are health information. Given that the ACS is the public health authority performing an intervention, the health information does not become individually identifiable. The public health authority is not listed as a collector of information in the definition of individually identifiable health information or protected health information. The release of patient identity and religious affiliation in the facility directory is an authorized protected health information disclosure. If the local faith-based organization leaders are established as State Department of Health volunteer employees, then they can provide services, otherwise this activity is disallowed.

### **Scenario 2: Analysis and Conclusions**

The evaluator uses the results from Step I and Step II to reach conclusions. Three privacy points have been identified:

1. Collection of health information from field staff
2. Possession and storage of medical information, collected as part of employee health screening activities
3. Release of information to supervisor, co-workers, and the media

Related to the collection of health information from field staff, employee medical information must be treated as a confidential medical record and access to that information must be limited. Related to possession and storage of medical information as part of employee health screening activities, that information must be collected and maintained in separate forms and in separate medical files. Those files cannot be made open to the public under the FOIA or the state law equivalent to FOIA. Releasing medical information to co-workers or to supervisors would not conform to law. However, supervisors and managers may be informed regarding necessary restrictions on the work or duties of employees, so release of work restriction would conform to law. Finally, releasing the number of ill public health employees in aggregate does not qualify as the release of medical records or patient identifying information.

## Step IV: Solutions

Once the evaluator has determined which privacy points conform to the law and which do not, he or she has useful information for creating solutions. Solutions could take several different forms:

- The activity can be conducted without modification.
- The activity must be modified to conform to federal and/or state law.
- The activity does not conform to federal and/or state law, but cannot be modified and therefore cannot be conducted.
- The activity does not conform to federal and/or state law, but it is possible, and advisable, to modify the law.

### **Scenario 1: Solutions**

The evaluator advises the ACS staff person to establish the local faith-based organization leaders as volunteer employees of the State Department of Health. The evaluator also recommends the creation of a plan for data protection, specifically storage, transmission, and disposal. Finally, the evaluator says that the religious affiliation of patients can be collected in a directory, as long as patients do not object.

### **Scenario 2: Solutions**

The evaluator informs the public health nurse that she cannot give the epidemiologist's medical information to his co-workers or supervisors. She can tell the supervisor if the epidemiologist should be out of work for seven days. She is also able to tell the reporter the number of sick employees, but should check with her supervisor first for approval.

<sup>1</sup> Centers for Disease Control and Prevention, US Department of Health and Human Services. Interim Pre-pandemic Planning Guidance: Community Strategic for Pandemic Influenza Mitigation in the United States—Early, Targeted, Layered Use of Nonpharmaceutical Interventions. February 2007. Available at: [http://www.pandemicflu.gov/plan/community/community\\_mitigation.pdf](http://www.pandemicflu.gov/plan/community/community_mitigation.pdf). Accessed: 07-10-07.

<sup>2</sup> Ibid.  
<sup>3</sup> Ibid.  
<sup>4</sup> Ibid.

## Acknowledgements

ASTHO would like to extend its thanks to the participants of the Privacy & Pandemic Flu Workshop who made this report possible. Special thanks to Rodney Johnson and Matthew Penn who provided the guide scenarios and valuable review and input, and to Jane Alm, Denise Chrysler, Gail Horlick, Robert Martin, and Eden Wells, who also contributed considerable time, effort, and expertise in the crafting of this report.

Workshop participants were:

**Jane Alm**

Privacy Officer  
Oregon Department of Human Services

**Brenda Carlson**

Chief Deputy  
San Mateo County Counsel

**Denise Chrysler**

Director, Office of Legal Affairs  
Michigan Department of Community Health Privacy  
Officer

**Glenda Ford-Lee**

Pandemic Influenza Coordinator  
Oklahoma State Department of Health

**Brant Goode**

CDC Career Epidemiology Field Officer Assignee  
to North Carolina  
North Carolina Division of Public Health

**Geoffrey Hoare**

Regional Preparedness Planning Coordinator  
Domestic Security Task Force Region 3  
Florida Department of Health

**Gail Horlick**

Privacy Rule Coordinator  
Office of Scientific Regulatory Services Office of  
the Chief Science Officer  
Centers for Disease Control and Prevention

**Rodney Johnson**

Chief Counsel and Privacy Officer  
Florida Department of Health

**Robert Martin**

HIPAA Coordinator  
North Carolina Division of Public Health

**Bruce McIntyre**

Deputy Chief of Legal Services  
Rhode Island Department of Health

**Toby L. Merlin**

Deputy Director, Influenza Coordination Unit  
Centers for Disease Control and Prevention

**Alysia Mihalakos**

Senior Public Health Promotion Specialist  
Rhode Island Department of Health

**Robn Mitchell**

HIPAA Privacy Officer  
Oklahoma State Department of Health

**Michael Morris**

Health Information Systems Coordinator  
HIPAA Privacy Officer  
West Virginia Bureau for Public Health

**Matthew S. Penn**

Staff Attorney  
South Carolina Department of Health and Environmental  
Control

**Julie Plagenhoef**

Public Health Preparedness Planner  
Oregon Department of Health

**Linda Sanches**

Senior Advisor, HIPAA Privacy Outreach & Training  
Office for Civil Rights  
US Department of Health & Human Services

**Cynthia Stamer**

Glast, Phillips, and Murray, P.C.

**Jennifer Stone**

Senior Assistant Attorney General  
Wyoming Attorney Generals Office

**Heather Theis**

Privacy Program Manager  
Wyoming Department of Health

**Eden Wells**

Medical Epidemiologist  
Pandemic Flu Coordinator  
Michigan Department of Community Health





(202) 371-9090 tel  
(202) 371-9797 fax  
2231 Crystal Drive  
Suite 450  
Arlington, VA 22202  
[www.astho.org](http://www.astho.org)  
Privacy & Pandemic Flu Guide  
NOVEMBER 2007  
PUB-0711005

Copyright © 2007 ASTHO.  
All rights reserved.