Permitted Uses and Disclosures: Exchange for Public Health Activities

45 Code of Federal Regulations (CFR) 164.512(b)(1)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities *without first obtaining* an individual's authorization. The Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR) previously issued fact sheets describing how this works when sharing PHI for treatment and for health care operations. This fact sheet explains, through hypothetical scenarios, how these rules work for disclosures of PHI for public health activities to **public health agencies that are authorized by state or federal law to collect the information they seek**. It also gives a few examples of sharing PHI in support of other important public health policies. While HIPAA requires that the information disclosed is the minimum information necessary for the purpose, it permits the discloser to reasonably rely on a public health authority's request as to what information is necessary for the public health activities.

Other laws may apply. This fact sheet discusses only HIPAA.

Depending upon the nature and manner of a disclosure, other requirements of the HIPAA Privacy and Security Rules may be applicable. For example, if a Business Associate (BA) discloses PHI for public health activities on behalf of a CE, the BA must be authorized to do so in the BA Agreement (BAA) it has with the CE. For any of the scenarios below in which electronic PHI is disclosed, the discloser must meet the HIPAA Security Rule requirements. All the scenarios apply to all types of CEs, whether they use health information technology (health IT) certified by ONC or other forms of electronic transmission.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 1: Exchange for Reporting of Disease

Healthy Hospital is located in the City of Sunshine, which has had a recent increase in the number of confirmed cases of the Zika virus.

The U.S. Centers for Disease Control and Prevention (CDC), acting in its capacity as a public health authority and authorized by law to collect disease surveillance information, requests that Healthy Hospital report PHI on an ongoing basis for all prior and prospective cases of patients exposed to the Zika virus, whether suspected or confirmed. Healthy Hospital may use health IT certified by the ONC Health IT Certification program ("certified health IT") to disclose PHI to the CDC in response to the request and may reasonably rely on CDC's request as to the PHI needed. Healthy Hospital must meet the requirements of the HIPAA Security Rule if providing electronic PHI to CDC. The CDC's ability to collect this type of information extends to all public health information within the scope of CDC's public health authority.

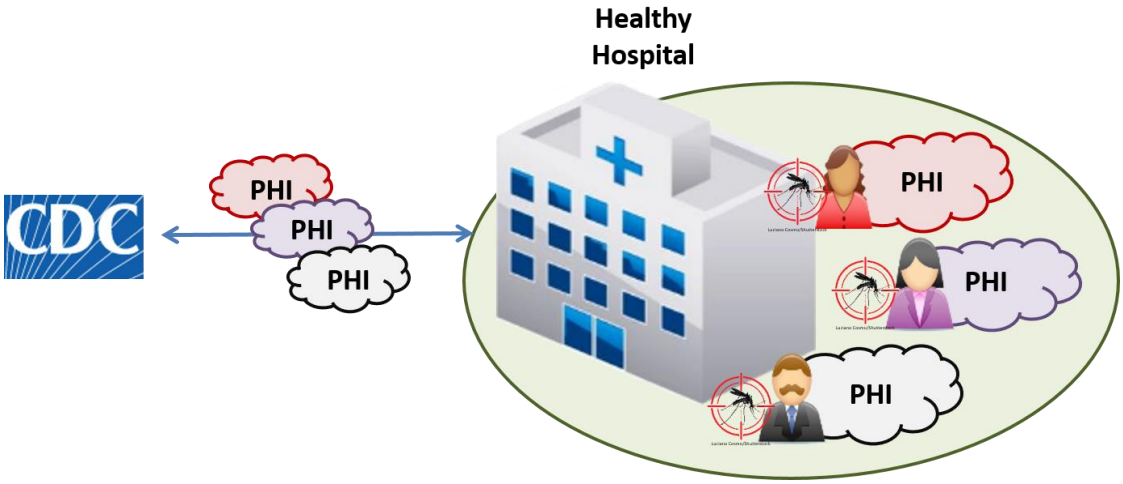

Figure 1: Reporting of Disease Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 2: Exchange for Conduct of Public Health Surveillance

Healthy Hospital is located in the State of Meadowvale. The Meadowvale Health Department maintains the state central cancer registry, and State law authorizes the Department to collect data on cancer occurrence (including the type, extent, and location of the cancer) and the type of initial treatment. Under 45 CFR 164.512(b)(1)(i), Healthy Hospital may use certified health IT to disclose electronic PHI to the Meadowvale Health Department's central cancer registry. In deciding how much and what information to supply to Meadowvale Department of Health, HIPAA permits Healthy Hospital to reasonably rely on the Meadowvale Department of Health's statement of what information is necessary for the public health activities. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

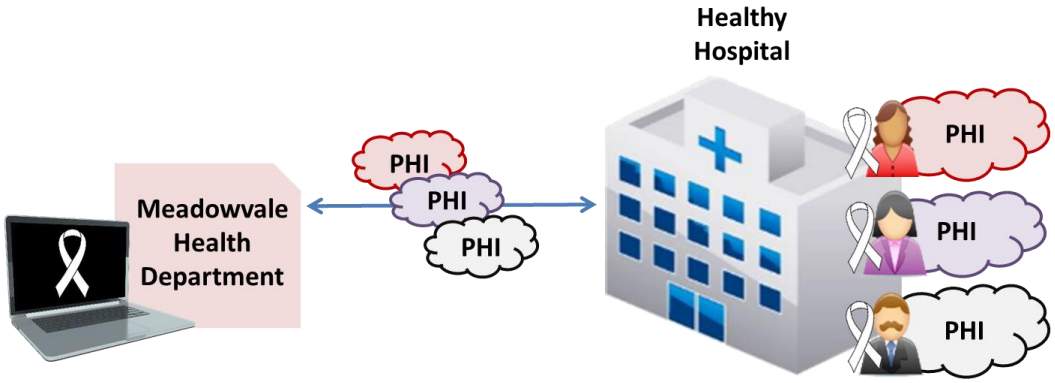

Figure 2: Public Health Surveillance Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 3: Exchange for Public Health Investigations

The State of Mountaintop Department of Health investigates the source of a recent measles outbreak in a local school, and State law authorizes the Department to access medical records to complete the investigations. The Mountaintop Department of Public Health asks all health providers in the state to report confirmed diagnoses of measles, including patient identity, demographic information, and positive test results. Under 45 CFR 164.512(b)(1)(i), providers within the State of Mountaintop may use certified health IT to disclose PHI to the Department of Health. While providers may only disclose the minimum necessary for the purpose of the public health investigation, they may reasonably rely on representations from the Department of Health about what PHI is necessary to conduct the investigation. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

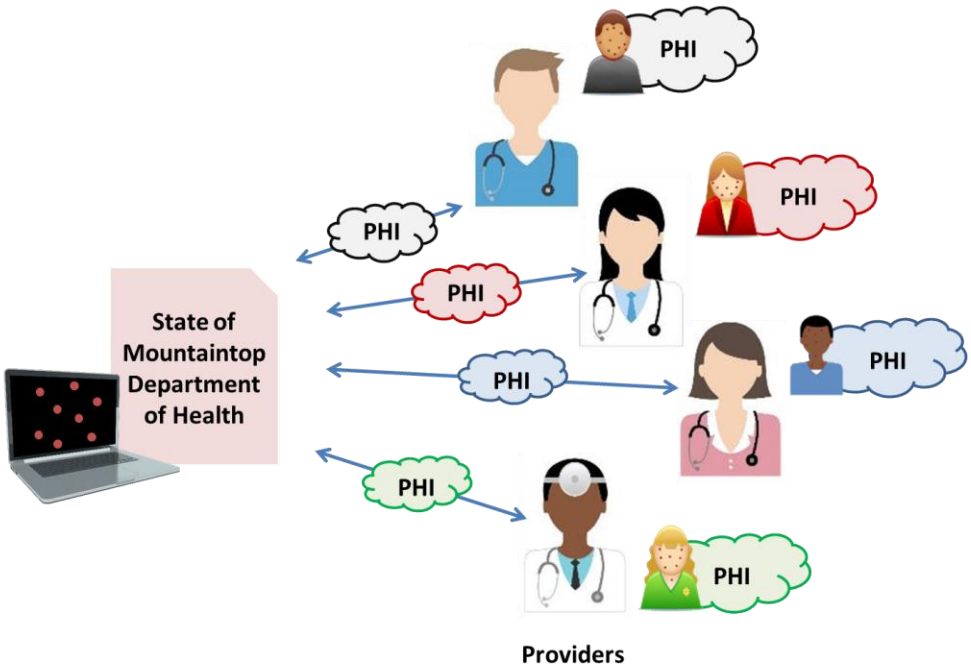

Figure 3: Public Health Investigations Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 4/5: Exchange for Public Health Interventions

When Urban City's water supply is found to be contaminated with lead in State Prariewind, the Prariewind Health Department implements a lead poisoning intervention program and needs lead exposure test results of children who might have been exposed. Because of the known long-term neurological effects of lead poisoning in children, Prariewind's Health Department is authorized by law to obtain the test results of each tested child and to track those children's health and development over time. The Department contracts with a local health information exchange (HIE) to collect, on the Health Department's behalf from local providers, PHI about the tested children. Under 45 CFR 164.512(b)(1)(i), providers may disclose the PHI to the Prariewind Health Department using certified health IT. While providers must only disclose the minimum necessary for the purpose of the public health intervention, they can reasonably rely on representations from the Prariewind Department of Health that the requested PHI is the minimum needed to implement the program. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

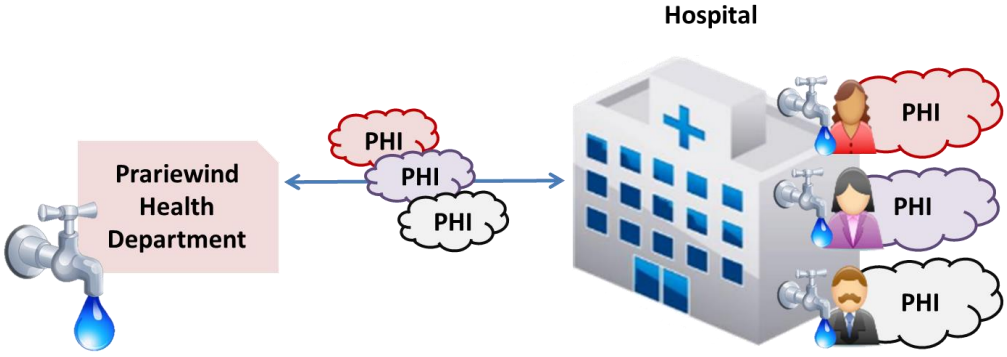

Figure 4: Public Health Interventions Scenario 1

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

For another example, the State of Coastalview Public Health Authority is responsible under state law for implementing a CMS State Innovation Model (SIM) program in their state. Coastalview was awarded a SIM grant to conduct a public health intervention measuring of outcomes for patients that have both diabetes and depression and whose primary care provider (PCP) coordinate their patients' care.

Coastalview requests that PCPs within the state disclose PHI to the state's Public Health Authority to assist in the evaluation of care coordination outcomes. Under 45 CFR 164.512(b)(1)(i), PCPs within Coastalview's jurisdiction may disclose PHI to the Coastalview Public Health Authority using certified health IT. While PCPs must only disclose the minimum necessary for the purpose of the public health intervention, they may reasonably rely on representations from the Public Health Authority that the requested PHI is the minimum needed. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

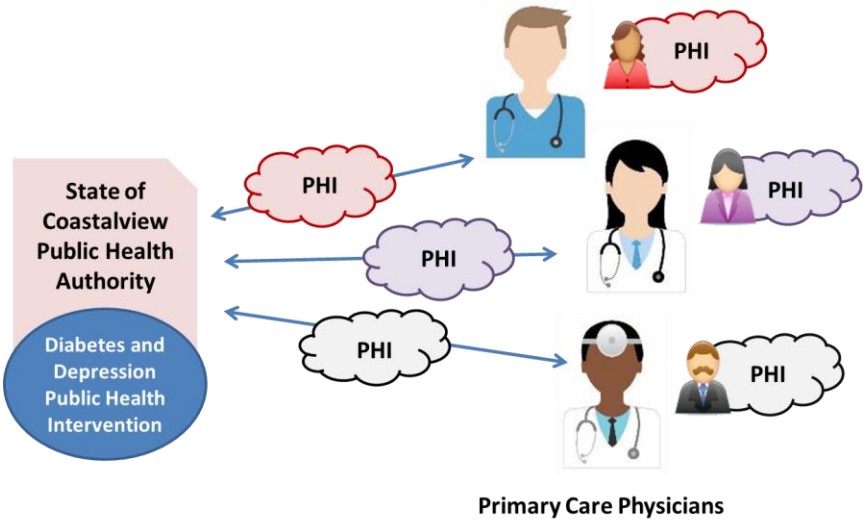

Figure 5: Public Health Interventions Scenario 2

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 6: Exchange Subject to Food and Drug Administration (FDA) Jurisdiction

Medical devices are subject to the jurisdiction of the U.S. Food and Drug Administration (FDA). A device manufacturer announces a Class I Medical Device Recall for HeartWare2.0. Dr. Johnson implanted HeartWare 2.0 in 35 patients prior to the recall. Dr. Johnson employs certified health IT to identify patients with HeartWare 2.0. She may disclose PHI, such as patient contact information and other health information about the affected patients, to the FDA under 45 CFR 164.512(b)(1)(iii)(c). Dr. Johnson must disclose only the information she thinks is necessary to support the recall, but she may seek the manufacturer's input, if she wants, in making that decision.

Disclosure of electronic PHI requires HIPAA Security Rule compliance.

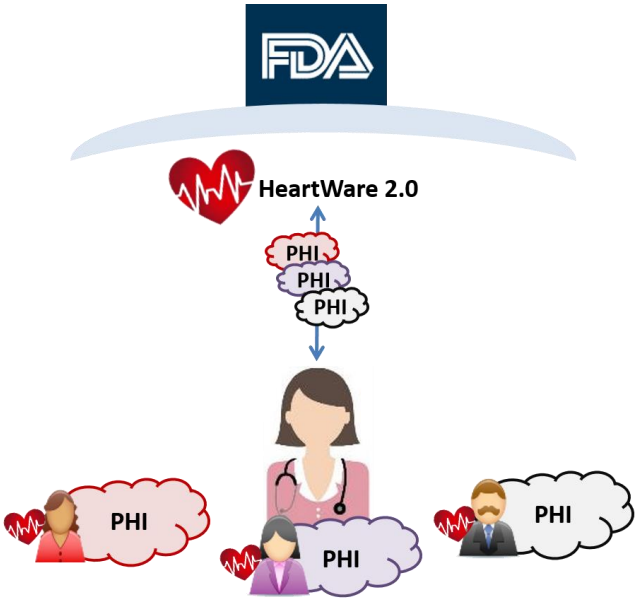

Figure 6: FDA Jurisdiction Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 7: Exchange for Persons Exposed to Communicable Disease and for Related Public Health Investigation

Patient Y went to the Emergency Department at Local Hospital due to a severe laceration to the leg. While in the waiting area, Patient Y sits next to Patient Z. It is later confirmed that Patient Z has an airborne, communicable virus. Patient Y and other patients in the waiting area were potentially exposed.

Local law permits providers to notify individuals that may have been exposed to a communicable disease. Local Hospital may use PHI and certified health IT to identify patients who were in the waiting area and potentially exposed to the virus. Local Hospital may send notices to the exposed patients about their exposure based on 45 CFR 164.512(b)(1)(iv). Local Hospital must only use and disclose the minimum necessary PHI for the purpose of the notification of exposure to the communicable disease.

Local Department of Health, in conjunction with Local Hospital, is conducting an investigation into outbreaks of the virus. Local Department of Health is authorized by law to collect disease information and access medical records to conduct investigations and implement disease control measures and asks Local Hospital to provide the PHI of patients exposed to the virus. Local Hospital may use certified health IT to disclose this PHI to the Department of Health based on 45 CFR 164.512(b)(1)(i). While Local Hospital must only disclose the minimum necessary for the purpose of the public health investigation, it may reasonably rely on the Local Department of Health's representations about what is the minimum information needed to conduct the investigation. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

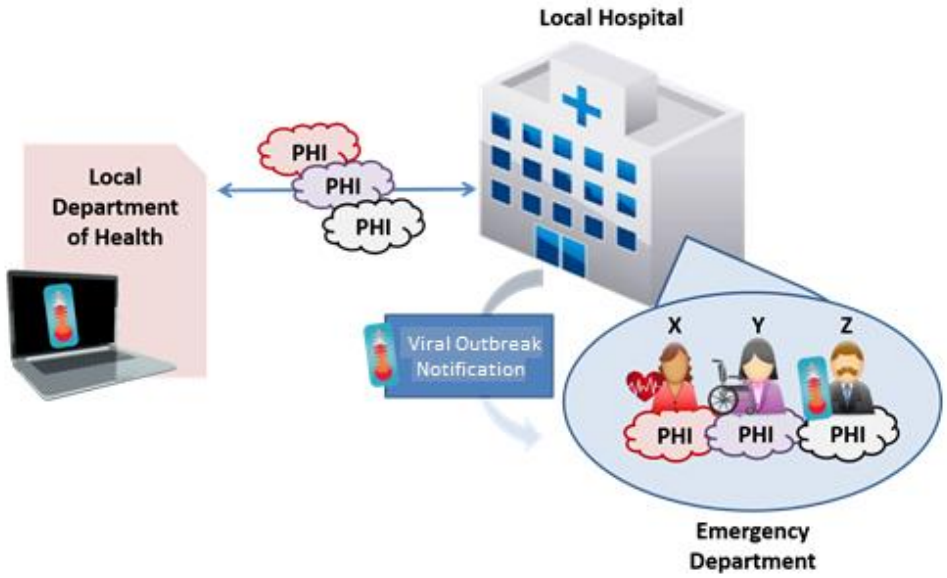

Figure 7: Exchange for Persons Exposed to Communicable Disease and for Related Public Health Investigations Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 8: Exchange in Support of Medical Surveillance of the Workplace

Worker Bee is employed by Mining 247 Company. By federal law, Mining 247 is required to monitor the safety of working conditions, also known as medical surveillance of the workplace. At the request of Mining 247 Company, Dr. Hopeful provides health care evaluation services to Worker Bee so the company can evaluate work-related illness and injuries and conduct medical surveillance. Mining 247 Company needs this information to comply with the Mine Safety and Health Administration (MSHA) and state laws. Under 45 CFR 164.512(b)(1)(v), Dr. Hopeful may disclose Worker Bee's workplace medical surveillance-related PHI to Mining 247 Company. Dr. Hopeful must provide Worker Bee with written notice that the information will be disclosed to his or her employer at the time the health care evaluation is provided (or the notice may be prominently posted at the worksite if that is where the service is provided). Dr. Hopeful must only disclose the minimum necessary PHI that consists of findings concerning the workplace surveillance. Dr. Hopeful discloses the information to Mining 247. As she disclosed the information electronically, the HIPAA Security Rule applies to her disclosure.

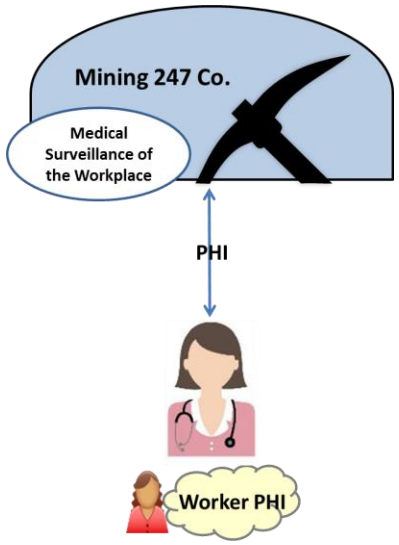

Figure 8: Exchange in Support of Medical Surveillance of the Workplace Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Scenario 9: Using Certified Electronic Health Record Technology

Providers who need to share PHI with agencies or organizations for public health activities may use certified health IT to send the information to the requesting agency or organization. Disclosure of electronic PHI by certified health IT or other electronic means requires HIPAA Security Rule compliance by the provider.

Additional Resources

- Office for Civil Rights HIPAA Regulations Website
- ONC Guide to Privacy & Security of Electronic Health Information (2015)[PDF-1.26MB]