Appendix F: HIPAA Waiver Toolkit

HIPAA Waivers for Disasters

Is the HIPAA Privacy Rule suspended during a national or public health emergency?

1. No.

2. CAUTION: State law may be much stricter than federal law
   a. Pre-emption analysis needs to be done regarding all of the exceptions below.
   b. The stricter law to protect privacy (whether federal or state) pre-empts.
   c. Thus in some states, the exceptions listed below will not be legal.

3. The Secretary of HHS may waive certain provisions of the Rule under the Project Bioshield Act of 2004 (PL 108-276) and Section 1135(b)(7) of the Social Security Act.

4. What provisions may be waived?
   a. If the President declares an emergency or disaster and the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the HIPAA Privacy Rule.
   b. Following are the waivable provisions:
      i. Patient's right to agree or object
         1. The requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care (45 CFR 164.510(b)).
         2. The requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a)).
      ii. Notice: The requirement to distribute a notice of privacy practices (45 CFR 164.520).
      iii. Restrictions by patients:
         1. The patient's right to request privacy restrictions (45 CFR 164.522(a)).

5. The patient's right to request confidential communications (45 CFR 164.522(b))
   When and to what entities does the waiver apply?

   a. If the Secretary issues such a waiver, it only applies:
      i. In the emergency area and for the emergency period identified in the public health emergency declaration.
      ii. To hospitals that have instituted a disaster protocol. The waiver would apply to all patients at such hospitals.
      iii. For up to seventy-two hours from the time the hospital implements its disaster protocol.

iv. In a pandemic infectious disease, the waiver is in effect until the termination of the declaration of the public health emergency.

b. When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if seventy-two hours has not elapsed since implementation of its disaster protocol.

c. Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations. For instance, the Privacy Rule allows covered entities (CEs) to share protected health information (PHI) with the American Red Cross so it can notify family members of the patient's location (45 CFR 164.510(b)(4)).

6. **Resource**: *See* Public Health Uses and Disclosures

Does the HIPAA Privacy Rule permit CEs to disclose protected health information, without individuals' authorization, to public officials responding to a bioterrorism threat or other public health emergency?

1. Yes.
   a. The Rule recognizes that various agencies and public officials will need PHI to deal effectively with a bioterrorism threat or emergency.
   b. To facilitate the communications that are essential to a quick and effective response to such events, the Privacy Rule permits CEs to disclose needed information to public officials in a variety of ways.

2. CEs may disclose PHI, without the individual's authorization, to a **public health authority** acting as authorized by law in response to a bioterrorism threat or public health emergency (*see* 45 CFR 164.512(b)), public health activities).

3. The Privacy Rule also permits a CE to disclose PHI to **public officials** who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism (*see* 45 CFR 164.512(j)), to avert a serious threat to health or safety).

4. In addition, disclosure of PHI, without the individual's authorization, is permitted:
   a. Where the circumstances of the emergency implicates law enforcement activities (*see* 45 CFR 164.512(f));
   b. National security and intelligence activities (*see* 45 CFR 164.512(k)(2)); or
   c. Judicial and administrative proceedings (*see* 45 CFR 164.512(e)).

5. **Resource**: *See* Disclosures in Emergency Situations

Can healthcare information be shared in a severe disaster?

1. Yes
2. Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all of the following ways:
    a. **Treatment:** Healthcare providers can share patient information as necessary to provide treatment, which includes.
        i. Sharing information with other providers (including hospitals and clinics);
        ii. Referring patients for treatment (including linking patients with available providers in areas where the patients have relocated); and
        iii. Coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).
    b. Providers can also share patient information to the extent necessary to seek **payment** for these healthcare services.
    c. **Notification**: Healthcare providers can share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.
        i. The healthcare provider should get verbal permission from individuals, when possible; but if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.
        ii. Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others as to the location and general condition of their loved ones.
        iii. In addition, when a healthcare provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.
    d. **Imminent Danger**: Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public—consistent with applicable law and the provider's standards of ethical conduct.
    e. **Facility Directory**: Healthcare facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.
3. Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.
4. **Resource**: *See* Disclosures Required by Law

When does the Privacy Rule allow CEs to disclose PHI to law enforcement officials?

1. The Privacy Rule is balanced to protect an individual's privacy while allowing important law enforcement functions to continue.
    a. The Rule permits CEs to disclose PHI to law enforcement officials, without the individual's written authorization, under specific circumstances.
    b. For a complete understanding of the conditions and requirements for these disclosures, providers need to review the exact regulatory text at the citations provided.
2. Disclosures for **law enforcement purposes** are permitted as follows:
    a. To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.
        i. The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information.
3. *See* 45 CFR 164.512(f)(1)(ii)(A)-(B).
    a. To respond to an **administrative request**, such as an administrative subpoena or investigative demand or other written request from a law enforcement official.
        i. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used 2) *See* 45 CFR 164.512(f)(1)(ii)(C).
    b. To respond to a request for PHI for purposes of identifying or locating a **suspect, fugitive, material witness or missing person**; but the CE must limit disclosures of PHI to name and address, date, and place of birth, social security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics.
        i. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request
        ii. *See* 45 CFR 164.512(f)(2).
4. This same limited information may be reported to law enforcement:
    a. About a **suspected perpetrator** of a crime when the report is made by the victim who is a member of the CEs workforce (45 CFR 164.502(j)(2)).
    b. To **identify or apprehend** an individual who has admitted participation in a violent crime that the CE reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512(j)(1)(ii)(A), (j)(2)-(3)).

5. To respond to a request for PHI about a **victim of a crime**, and the victim agrees.
    a. If, because of an emergency or the person's incapacity, the individual cannot agree, the CE may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the CE believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512(f)(3)).

6. Where **child abuse victims or adult victims of abuse, neglect, or domestic violence** are concerned, other provisions of the Rule apply:
    a. Child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512(b)(1)(ii)).
    b. Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such reports (45 CFR 164.512(c)):
        i. If the individual agrees;
        ii. If the report is required by law; or
        iii. If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (*see* 45 CFR 164.512(c)(1)(iii)(B)).
        iv. Notice to the individual of the report may be required (*see* 45 CFR 164.512(c)(2)).

7. To report PHI to **law enforcement** when required by law to do so.
    a. *See* 45 CFR 164.512(f)(1)(i).
    b. For example, state laws commonly require healthcare providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.

8. To alert law enforcement to the **death** of the individual.
    a. When there is a suspicion that death resulted from criminal conduct (*see* 45 CFR 164.512(f)(4)).
    b. Information about a decedent may also be shared with medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties (45 CFR 164.512(g)(1)).

9. To report PHI that the CE in good faith believes to be evidence of a **crime** that occurred on the CEs premises (45 CFR 164.512(f)(5)).

10. When responding to an **off-site medical emergency**, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime.

a. *See* 45 CFR 164.512(f)(6).
b. This provision does not apply if the CE believes that the individual in need of the emergency medical care is the victim of abuse, neglect, or domestic violence.

11. When consistent with **applicable law and ethical standards**:

    a. To a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public (45 CFR 164.512(j)(1)(i)); or
    b. To identify or apprehend an individual who appears to have escaped from lawful custody (45 CFR 164.512(j)(1)(ii)(B)).

12. For certain other **specialized governmental law enforcement purposes**, such as:

    a. To federal officials authorized to conduct intelligence, counter- intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));
    b. To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody of an inmate or others if they represent such PHI is needed to provide healthcare to the individual; for the health and safety of the individual, other inmates, officers, or employees or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

13. Except when required by law, the disclosures to law enforcement summarized above are subject to a **minimum necessary** determination by the CE (45 CFR 164.502(b), 164.514(d)).

    a. When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)).
    b. Moreover, if the law enforcement official making the request for information is not known to the CE, the CE must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)).

14. **Resource**: *See* Disclosures for Law Enforcement Purposes

DISCLOSURES FOR PUBLIC HEALTH ACTIVITIES (45 CFR 164.512(b))

Background

1. The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to PHI to carry out their public health mission.

2. The Rule also recognizes that public health reports made by CEs are an important means of identifying threats to the health and safety of the public at large, as well as individuals.

3. The Rule permits CEs to disclose PHI without authorization for specified public health purposes.

How the Rule Works

1. General Public Health Activities.
    a. The Privacy Rule permits CEs to disclose PHI, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability (*see* 45 CFR 164.512(b)(1)(i)). This would include, for example,
        i. The reporting of a disease or injury;
        ii. Reporting vital events, such as births or deaths; and
        iii. Conducting public health surveillance, investigations, or interventions.
    b. Also, CEs may, at the direction of a public health authority, disclose PHI to a foreign government agency that is acting in collaboration with a public health authority (*see* 45 CFR 164.512(b)(1)(i)).
    c. CEs who are also a public health authority may use, as well as disclose, PHI for these public health purposes (*see* 45 CFR 164.512(b)(2)).
        i. A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency (*see* 45 CFR 164.501).
        ii. Examples of public health authorities include:
            1. State and local health departments;
            2. The Food and Drug Administration (FDA);
            3. The Centers for Disease Control and Prevention (CDC); and
            4. The Occupational Safety and Health Administration (OSHA).

2. Generally, CEs are required reasonably to limit the PHI disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose.
    a. CEs are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law (*see* 45 CFR 164.502(b)).
    b. For disclosures to a public health authority, CEs may reasonably rely on a minimum necessary determination made by the public health authority in requesting the PHI (*see* 45 CFR 164.514(d)(3)(iii)(A)).
    c. For routine and recurring public health disclosures, CEs may develop standard protocols, as part of their minimum necessary policies and procedures, that address the types and amount of PHI that may be disclosed for such purposes (*see* 45 CFR 164.514(d)(3)(i)).

3. Other Public Health Activities.

    a. The Privacy Rule recognizes the important role that persons or entities other than public health authorities play in certain essential public health activities.
    b. Accordingly, the Rule permits CEs to disclose PHI, without authorization, to such persons or entities for the public health activities discussed below.
    c. **Child abuse or neglect**. CEs may disclose PHI to report known or suspected child abuse or neglect, if the report is made to a public health authority or other appropriate government authority that is authorized by law to receive such reports.
        i. For instance, the social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case, the Privacy Rule would permit a CE to report such cases to that authority without obtaining individual authorization.
        ii. Likewise, a CE could report such cases to the police department when the police department is authorized by law to receive such reports (*see* 45 CFR 164.512(b)(1)(ii)).
    d. **Quality, safety, or effectiveness of a product or activity regulated by the FDA.** CEs may disclose PHI to a person subject to FDA jurisdiction, for public health purposes related to the quality, safety, or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples of purposes or activities for which such disclosures may be made include, but are not limited to:
        i. Collecting or reporting adverse events (including similar reports regarding food and dietary supplements), product defects or problems (including problems regarding use or labeling), or biological product deviations;
        ii. Tracking FDA-regulated products;
        iii. Enabling product recalls, repairs, replacement, or lookback (which includes locating and notifying individuals who received recalled or withdrawn products or products that are the subject of lookback); and
        iv. Conducting post-marketing surveillance.

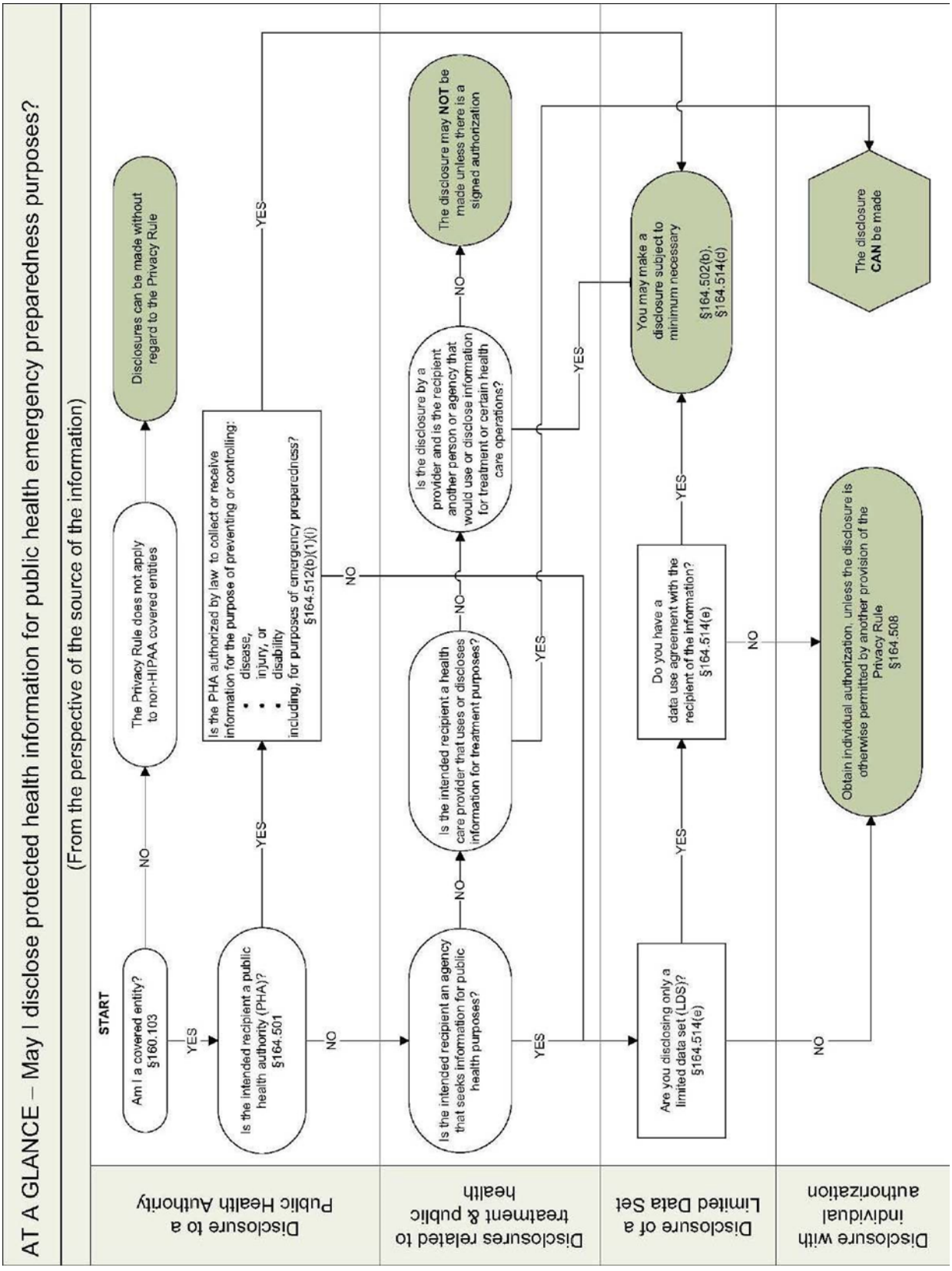
v. The "person" subject to the jurisdiction of the FDA does not have to be a specific individual.
    1. Rather, it can be an individual or an entity, such as a partnership, corporation, or association.
    2. CEs may identify the party or parties responsible for an FDA-regulated product from the product label, from written material that accompanies the product (known as labeling), or from sources of labeling, such as the Physician's Desk Reference.
    3. *See* 45 CFR 164.512(b)(1)(iii).

e. **Persons at risk of contracting or spreading a disease**. A CE may disclose PHI to a person who is at risk of contracting or spreading a disease or condition if other law authorizes the CE to notify such individuals as necessary to carry out public health interventions or investigations.
    i. For example, a CE may disclose PHI as needed to notify a person that (s)he has been exposed to a communicable disease if the CE is legally authorized to do so to prevent or control the spread of the disease.
    ii. *See* 45 CFR 164.512(b)(1)(iv).

f. Workplace medical surveillance.
    i. A CE who provides a healthcare service to an individual at the request of the individual's employer, or provides the service in the capacity of a member of the employer's workforce, may disclose the individual's PHI to the employer for the purposes of workplace medical surveillance or the evaluation of work-related illness and injuries to the extent the employer needs that information to comply with OSHA, the Mine Safety and Health Administration (MSHA), or the requirements of State laws having a similar purpose.
    ii. The information disclosed must be limited to the provider's findings regarding such medical surveillance or work-related illness or injury.
    iii. The CE must provide the individual with written notice that the information will be disclosed to his or her employer (or the notice may be posted at the worksite if that is where the service is provided) (*see* 45 CFR 164.512(b)(1)(v)).

Resources and Frequently Asked Questions

1. Privacy Rule FAQs
2. General information on Privacy of Health Information/HIPAA


AT A GLANCE – May I disclose protected health information for public health emergency preparedness purposes?
(From the perspective of the source of the information)
Disclosure to a Public Health Authority
Disclosures related to treatment & public health
Disclosure of a Limited Data Set
Disclosure with individual authorization
START
Am I a covered entity? §160.103
NO
YES
The Privacy Rule does not apply to non-HIPAA covered entities
Disclosures can be made without regard to the Privacy Rule
Is the intended recipient a public health authority (PHA)? §164.501
YES
NO
Is the PHA authorized by law to collect or receive information for the purpose of preventing or controlling:
• disease,
• injury, or
• disability
including, for purposes of emergency preparedness? §164.512(b)(1)(i)
YES
NO
Is the intended recipient an agency that seeks information for public health purposes?
NO
YES
Is the intended recipient a health care provider that uses or discloses information for treatment purposes?
NO
YES
Is the disclosure by a provider and is the recipient another person or agency that would use or disclose information for treatment or certain health care operations?
NO
YES
The disclosure may NOT be made unless there is a signed authorization
Are you disclosing only a limited data set (LDS)? §164.514(e)
YES
NO
Do you have a data use agreement with the recipient of the information? §164.514(e)
YES
NO
You may make a disclosure subject to minimum necessary §164.502(b), §164.514(d)
Obtain individual authorization, unless the disclosure is otherwise permitted by another provision of the Privacy Rule §164.508
The disclosure CAN be made