Preparation

Ensure that you formally assign responsibility, document response policies and procedures, establish an incident response team, share accurate contact information, and train your incident handlers.

Identification

Begins when defenders discover signs of an incident. Identify all affected systems.

Containment

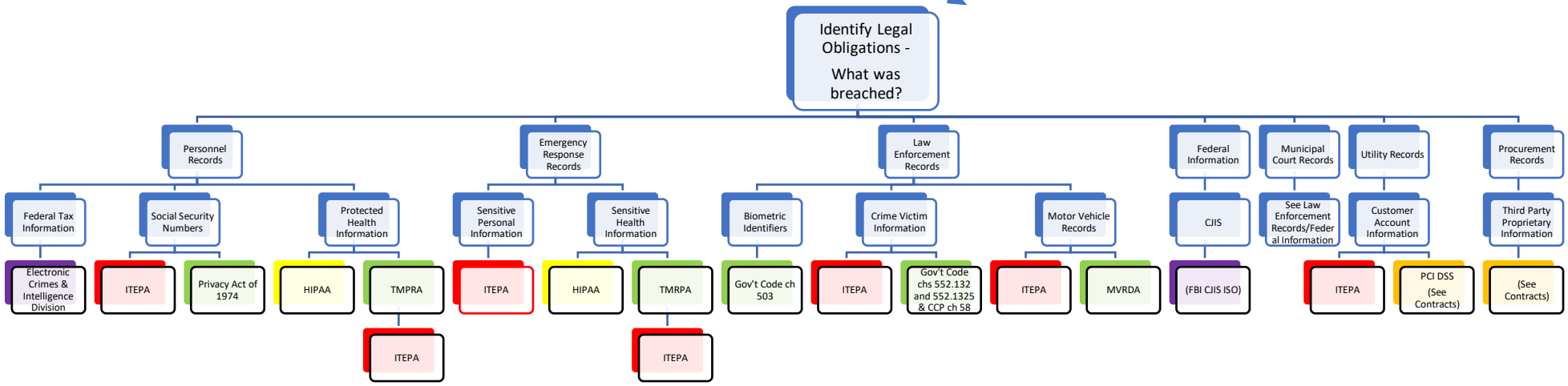
Once the Incident Handler has determined which systems are affected and the potential impact, move to the containment phase. Preserving evidence whenever possible. Analyze collected evidence (disk images, memory dumps, network logs) to create a full timeline of the incident. This vital step ensures the incident has been fully contained and will aid in the recovery phase.

Recovery

Compromised systems should be rebuilt, affected customers should be notified, and attack vectors identified during the Identification and Containment phases should be remediated.

Post Incident

Assess and improve the incident response process. During this phase, the notes, Incident Handler's notes, timeline of the incident, evidence collected, and any other information about the incident should be archived.



Type of Records

ITEPA Breach Notification

HIPAA Breach Notification

Notify Agency

Contractual Breach Notifications

Regulated Records

HIPAA - PHI not subject to encryption safe harbor

- **Individual Notice**
  - Written form: first class mail or email, if individual has agreed to electronic notice
  - Must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach
  - Must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach, and must include:
    - a brief description of the breach;
    - a description of the types of information that were involved in the breach;
    - the steps affected individuals should take to protect themselves from potential harm;
    - a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
    - contact information for the covered entity (or business associate, as applicable).
- **Media (>500 residents)**
  - Must provide notice to prominent media outlets serving the state or jurisdiction
  - May be in the form of a press release to appropriate media outlets serving the affected area
  - Must be provided without unreasonable delay, and in no case later than 60 days following the discovery of a breach, and must include the same information required for the individual notice
- **Secretary**
  - Notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form
  - Breach affects ≥500 individuals, city must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach
  - Breach affects <500 individuals, the city may notify the Secretary of such breaches on an annual basis
    - Reports of breaches affecting <500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered
- **Business Associate Experiences Breach**
  - Must provide notice to the city without unreasonable delay and no later than 60 days from the discovery of the breach
  - Business associate should provide the city with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals
- **Administrative Requirements and Burden of Proof**
  - City should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required because:
    - its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or
    - the application of any other exceptions to the definition of "breach."
  - Must have in place written policies and procedures regarding breach notification;
  - Must train employees on these policies and procedures; and
  - Must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

Identity Theft Enforcement and Protection Act

- **Individual**
  - Must provide written notice at the last known address of the individual
    - Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001, Consumer disclosures; or
    - If the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:
      - electronic mail, if the person has electronic mail addresses for the affected persons;
      - conspicuous posting of the notice on the person's website; or
      - notice published in or broadcast on major statewide media.
  - Disclosure must be made without unreasonable delay and in each case not later than the 60th day after the date on which the city determines that the breach occurred
    - Delay is okay if to determine the scope of the breach and restore the reasonable integrity of the data system; or
    - is at the request of a law enforcement agency that determines that the notification will impede a criminal investigation.
  - Resident of another state that has a breach notification law may receive notification under that state's law
  - A city that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under ITEPA complies if the city notifies affected persons in accordance with that policy
- **Consumer Reporting Agency (>10,000 persons)**
  - Must notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices
  - The city shall provide the notice required by this subsection without unreasonable delay
- **Attorney General (≥250 persons)**
  - Must notify the attorney general not later than the 60th day after the date on which the city determines that the breach occurred if the breach involves at ≥250 residents of this state
  - Notice must include:
    - a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
    - the number of residents of this state affected by the breach at the time of notification;
    - the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
    - the measures taken by the person regarding the breach;
    - any measures the person intends to take regarding the breach after the notification is given; and
    - information regarding whether law enforcement is engaged in investigating the breach.