

HIPAA Results

HIPAA Report Data

The InterLynx Security Database outputs beautiful color reports that detail the entire interview process, including color-coded ratings, full standard descriptions, and a complete record of the questions and answers from interview candidates. An example of the report entry format is shown below:

Example Report Entry

Administrative Safeguard	
Area:	Assigned Security Responsibility
HIPAA Standard:	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Goal:	Assign and Document the Individual's Responsibility
Citation:	164.308(a)(2) <input checked="" type="checkbox"/> Required <input type="checkbox"/> Addressable
Recommendations:	<ul style="list-style-type: none">• Document the assignment to one individual's responsibilities in a job description.• Communicate this assigned role to the entire organization.
Question	
Have the staff members in the organization been notified as to whom to call in the event of a security problem?	
Answer	
Yes. Tom Donahue is the primary contact.	

The area outlined in black describes the major HIPAA category of security safeguards, which are defined in the HIPAA Security Rule. These safeguards are classified as Administrative, Physical, or Technical.

Example HIPAA Category Header

Administrative Safeguard
Area: Assigned Security Responsibility
HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

Annotations with arrows pointing to the table:

- HIPAA Control Category points to "Administrative Safeguard"
- HIPAA Control Type points to "Assigned Security Responsibility"
- HIPAA Control Definition points to "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

Administrative safeguards are defined by the Security Rule as the “administrative actions and policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.”

Physical safeguards are defined as controls that are “physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

Technical safeguards are “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”


There are also two other safeguard categories which are self-explanatory:

- 1) Policies, Procedures and Documentation Requirements
- 2) Organizational Requirements

The HIPAA control type is a subcategory of the safeguard and helps to further clarify the area of responsibility for the covered entity. The HIPAA control definition describes the control type and describes what is needed to do to comply in each area.





Below each category header is a section that details the specification goal(s) of each area, and some other useful information. An example of the specification header is show below:

Example Specification Area

Compliance Indicator		Required by Covered Entity	Addressable by Covered Entity
	Goal:	Assign and Document the Individual's Responsibility	
	Citation:	164.308(a)(2)	<input checked="" type="checkbox"/> Required <input type="checkbox"/> Addressable
	Recommendations:	<ul style="list-style-type: none"> • Document the assignment to one individual's responsibilities in a job description. • Communicate this assigned role to the entire organization. 	

The header includes the direct citation from the HIPAA Security Rule official document published by the U.S. Center for Medicare & Medicaid Services (CMS). The Compliance Indicator is a quick reference tool that is used to gauge the level of compliance to each Security Rule specification.

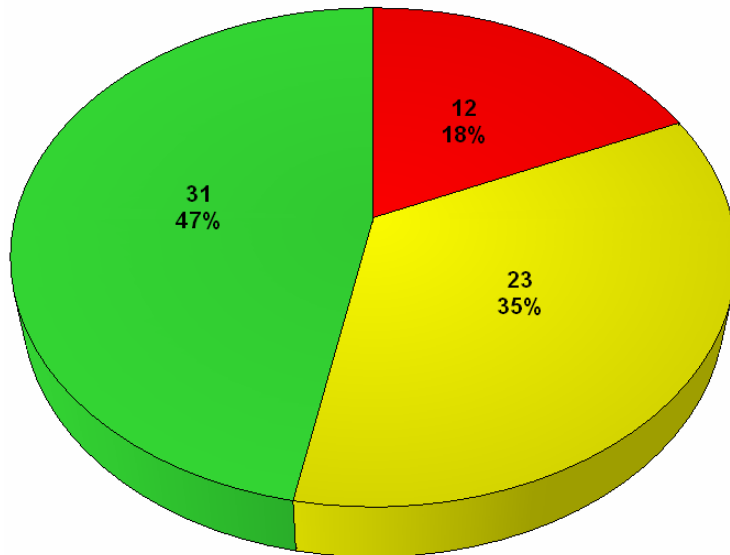
Example Compliance Indicators

-  Information or topic not addressed during the interview
-  Estimated compliant
-  Indicates partial compliance
-  Indicates areas needing attention

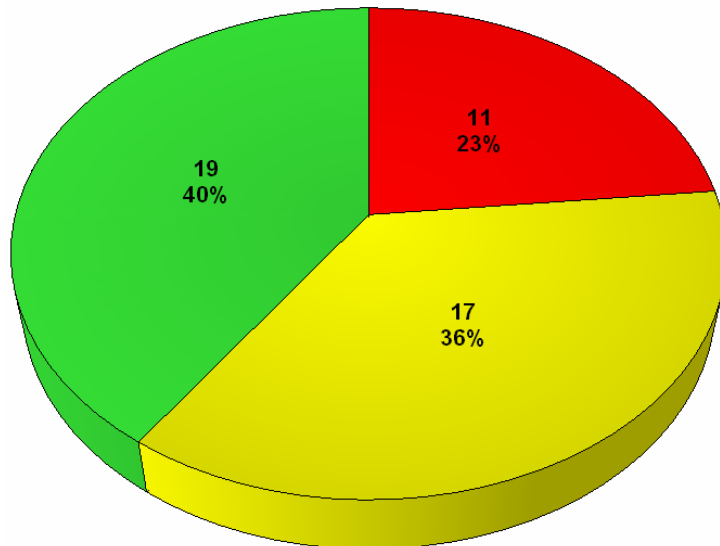
HIPAA Compliancy Summary Graphs

The following graphs are also included with the HIPAA database, and can be generated for inclusion in reports or presentations.

Overall HIPAA Safeguard Compliancy



Compliancy To HIPAA Required Standards



Compliance By Safeguard Type

