OIX-2 Data Center Standards / HIPAA Crosswalk

In the world of Health Information Technology, compliance with the HIPAA regulations is in the forefront for both large and small healthcare organizations. HIPAA compliance means having technical, physical and administrative controls in place to protect the availability, integrity, and confidentiality of patient information.

Data Center operators who service the Healthcare industry must demonstrate compliance with components of HIPAA directly related to their scope of responsibility. This document identifies the Open-IX standards and how they cross over specific aspects of HIPAA they're responsible for.

Customers of OIX-2 certified facilities can utilize this document to understand how the certified operator is addressing HIPAA regulations. In particular, it outlines what specific HIPAA requirements the operator may be responsible for via a Business Associate Agreement (BAA), Contract, or SLA, ensuring scope is appropriately limited.

Under the HIPAA Requirements, a covered entity must address issues that relates to

- Confidentiality
- Accessibility
- Integrity

Of Protected Health Information

OIX-2 Data center Standards / HIPPA Crosswalk:

Open IX standard	HIPAA Crosswalk Section	Comments
Physical Requirements		

Utility Feeds	Availability	Redundancy in Utility Feeds helps to protect the availability of Patient Data
Utility Transformers	Availability	N+1 is vital in protecting the availability of data
Water Sources	Availability	This is necessary to protect the availability and functionality of the data center
Network Access	Availability	Diverse network connectivity is vital in protecting the availability of data
Meet Me Room	Availability	Network security and segmentation is vital in protecting the availability and security of data
Interconnection Service Delivery		There is no HIPAA crosswalk
Electrical Distribution		N+1 is vital in protecting the availability of data
Generator	Availability	Redundancy in Power is vital to protect the availability of Patient Data
UPS	Availability	Redundancy in Power is vital to protect the availability of Patient Data
Cooling	Availability	Redundancy in Power is vital to protect the availability of Patient Data
Floor Load	Availability	A solid physical construction is vital in protecting the data center from physical damage and protecting the availability of data
Flood Zone	Availability	Having controls in place that address environmental risks are an important part of insuring availability of patient data

Seismic Zone	Availability	Having controls in place that address environmental risks are an important part of insuring availability of patient data
Tornado / Hurricane Zone	Availability	Having controls in place that address environmental risks are an important part of insuring availability of patient data
Adjacent Transportation		There is no HIPAA crosswalk
Adjacent Hazards	Availability	Having controls in place that address environmental risks are an important part of insuring availability of patient data
Fire Protection	Integrity	In case of Fire, clean automatic shutdown of all servers is vital in protecting the integrity of hardware, software and data
Security	Confidentiality	Security is a vital control to ensure that unauthorized individuals to not have access to patient data. The controls listed should be enhanced to include logging of all visitors and escort of visitors at all times when in the data center.
Operational Requirements		
Rules	Confidentiality	Having a set of policies and procedures that relates to HIPAA compliance is necessary for a Data Center that hosts Protected health Information
Licensing		There is no HIPAA crosswalk
Commissioning		There is no HIPAA crosswalk

Maintenance	Availability	Maintenance of the data center support and backup systems is vital to maintaining Availability of the Data. This should be enhanced to include patch policies on all network devices such as switches.
Operating Procedures		Refer to Policies and Procedures addressed in the Rules Section
Hours of Operation	Availability and Integrity	Providers must have 24/7 access to their data. Therefore 24/7 access to the data center is required to allow for emergency access to the data for emergency maintenance to hardware or to access data during down times at medical facilities.
Change Management	Confidentiality, Availability and Integrity	Logging of all infrastructure changes is a vital part of the administrative HIPAA measures providers must comply with. This logging will demonstrate proper reactions to potential threats to data.
Workflow Management	Confidentiality, Availability and Integrity	Proper procedures and systems is a vital part of the administrative HIPAA measures providers must comply with. Standard operating procedures demonstrate proper reactions to potential threats to data and help ensure data availability.
Disaster Plan	Availability	Disaster Recovery is a vital aspect of each and every HIPAA compliance plan. In addition to the plan being in place it needs to be tested and reviewed regularly to ensure that if it is activated in a disaster it will work.
Communication		Business Associate Agreements mandate communication between the data center and the

		owner of the data at the time of an identified HIPAA Breach
Compliance		There is no HIPAA crosswalk
Environmental Compliance		There is no HIPAA crosswalk
Energy Conservation		There is no HIPAA crosswalk