HIPAA Compliance Check Report

Compliance Check Results

Check	*Description*	*Result*	*Remedy (if failed)*
SSH connection	Ensure that the SSH connection to the server is secure and functioning.	**Passed**	N/A
MySQL connection	Ensure that the system can connect to the MySQL database where patient data is stored.	**Failed**	Check the database credentials and ensure the MySQL server is running. Verify network access to the database.
HIPAA privacy policy	Verify that the HIPAA privacy policy exists and is accessible to users.	**Failed**	Ensure that the HIPAA privacy policy is uploaded to the server and placed in the correct directory. Check permissions to make it accessible.
Encryption of PHI	Ensure that encryption is enabled for sensitive patient data in the database.	**Failed**	Configure SSL encryption for MySQL and other databases. Ensure the appropriate settings are in place.
User access control	Ensure proper user access controls are in place to protect PHI.	**Failed**	Implement role-based access control (RBAC) to limit access to PHI based on user roles.
Data breach response plan	Ensure that a data breach response plan is in place.	**Failed**	Develop a data breach response plan, including detection and notification procedures, and store it on the server.
Audit logs for PHI access	Ensure that audit logs for access to PHI are maintained.	**Failed**	Implement logging mechanisms to track access to PHI and regularly review these logs.
Employee training on HIPAA	Ensure that employees are trained on HIPAA compliance and the handling of PHI.	**Passed**	N/A