This is a summary document with content provided by eMDS.

Please call CHS 800.250.8687 for assistance.

eMDs/CHS Core Customer Messaging

Customers need to stay compliant with HIPAA security requirements.

If a practice completes their Security Risk Assessment and has End of Life software, this is a potential HIPAA violation.

Http://www.hhs.gov/sites/default/files/June-2018-newsletter-software-practices.pdf

eMDs and CHS is offering an opportunity to get current with SQL now, rather than waiting until Fall sales period for upgrades.

Stress Involved Risks. Customers still running on an old database and old Operating System probably also have older computer equipment. This increases security risks. Old databases and Operating Systems are not supported by Microsoft and vulnerable to hacking and viruses. Don't risk and time out of security compliance. Move up to the new Lytec now.

Background on Unsupported SQL Versions

The end of Microsoft Support for SQL 2008R2 was July 9, 2019 so it is necessary to upgrade to a newer Lytec version to install SQL 2012 and remain within continued support and HIPAA security compliance.

If a security vulnerability is discovered Microsoft will NOT release a patch to fix it. Therefore, any computer or program out-of-date will no longer fully be protected and is no longer HIPAA-compliant.

Lytec 2011 through 2014 shipped with MS SQL 2008 (both Express and Standard versions).

Lytec 2015 and higher shipped with MS SQL 2012 (both Express and Standard versions). Customers need to verify that Lytec is actually running SQL 2012 since a simple upgrade performed would NOT have replaced the old SQL 2008 version.

Why Stay Current – HIPAA Requires It

Old versions are often specifically targeted and exploited by cyber criminals. The WannaCry ransomware attack of 2017 showed 98 percent of affected businesses used an outdated version of their Operating System. (Source: Kaspersky Labs May 2017)

The Security Rule under HIPAA mandates requirements for information systems that contain electronic protected health information. As part of the information system, the security capabilities of the operating system may be used to comply with technical safeguards. Any known security vulnerabilities of an operating system should be considered in the covered entity's risk analysis. An example of this

would be if the operating system is no longer supported by its manufacturer. (Source: Health and Human Services Office for Civil Rights)

Under the HIPAA Security Rule 45 C.F.R. 164.308 (a) (5) (ii), organizations must implement procedures for detecting, guarding against, and reporting malicous software. If you are using software that Microsoft no longer supports, providers will not meet the requirements for HIPAA compliance.