Health Information Compliance Alert

Not Sure Whether Encryption's For You? 4 Examples Will Help You Decide

Using the five variables enumerated by **Jim Sheldon-Dean** (see article "Tales From Encryption: Don't Turn E-mail Security Into A Horror Story") with **Lewis Creek Systems** in Charlotte, VT, take a look at these four examples featuring how an entity might decide to encrypt - or not to encrypt - its e-mail transmissions:

Example #1: For a dental appointment reminder sent over the Internet, you'd have low criticality, very incomplete information, and data for only one person. Required protection would be limited to that provided in Internet e-mail, (i.e., password-protected access to accounts), but no encryption would be required.

Example #2: For a file of patient records for all patients of a certain demographic being sent by Internet to a business associate to be mined for additional Medicare or Medicaid dollars, you'd have medium criticality, high completeness, and many people. You would want to be sure the information was accurate and unmodified for such work, so both encryption and integrity controls would be indicated (If sent by a dial-up line, encryption would not be required).

Example #3: For most communications within a facility on a protected network, or communicating by a dedicated, circuit-switched line, the adoption of properly used and enforced access controls will be sufficient to protect against unauthorized access. However, for some communications that may be subject to more restrictive regulation, such as mental health, drug abuse, or HIV information (high criticality), encryption of communication within the facility may be indicated.

Example #4: For professional communications over the Internet, such as between covered entities and between CEs and business associates, the organizational capability of professionals should be such that encryption be provided, even when the number of patients, completeness, and criticality may be low.