Use of Encryption

Sensitive data that is protected with encryption technology is meaningless to anyone who does not possess the encryption key. Encryption is the process of converting information (either at-rest in a database or in-transit to another party) into code. This code is unintelligible to anyone who is not in possession of the corresponding encryption key to translate the code back to readable information. This means that if the data is lost or stolen, there may not have been a “breach” depending upon applicable federal or state law (provided that the encryption key was not also taken). HIPAA regulations provide for safe harbor to institutions who can demonstrate that lost or stolen PHI was in an encrypted format. This is particularly important for mobile devices and portable media such as laptops, tablets, phones with locally stored information, and portable drives containing PII - as they have a tendency to go missing regularly.