Personally Identifiable Information (PII) Data Questions

Storing and Retrieving Personally Identifiable Information in TEKWave Software

Overview and Purpose

This document is designed to help you the customer understand how TEKWave addresses the issue of privacy and compliance regarding Personally Identifiable Information (PII).

PII is defined as:

> Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Another term similar to PII, "personal information" is defined in a section of the California data breach notification law, SB1386:

> (e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Though the laws vary from state to state, the common factor amongst most states is that PII must be:

- encrypted or masked at the database level
- presented in an unreadable/non-viewable format on a screen
- presented in an unreadable/non-viewable format on a report

Data and Questions

Regarding TEKWave software the following components of PII addressed are:

1. Legal Name
2. Drivers License Number
3. DoB (Date of Birth)
4. Encryption

1. Legal Name:
    a. Can the complete name be recorded? Yes
    b. Is it required that the name be encrypted in the database? No

   c. Is it required that the name be masked when viewed or printed? No
2. Drivers License Number
   a. Can the complete number be recorded? Yes
   b. Is it required that the number be encrypted in the database? Yes, either encrypted or masked
   c. Is it required that the number be masked when viewed or printed? Yes
   d. If it must be masked, how much must be masked? Entire number is encrypted and masked in the TEKWave database
   e. If it must be masked, are there any exceptions when it is acceptable or desired to not mask the information, as in filing a criminal charge?
      i. The business area should have the ability to unencrypt or unmask at the DB level if an investigation is initiated
         1. TEKWave will assist in unmasking when required
3. Date of Birth
   a. Can the completed date be recorded? Yes
   b. Is it required that the date be encrypted in the database?
      i. TEKWave encrypted the year
   c. Is it required that the date be masked when viewed and/or printed?
      i. Yes, TEKWave encrypts the year
   d. If it must be masked how much must be masked?
      i. Year only
   e. If it must be masked, are there any exceptions when it is acceptable or desired to not mask the information, as in filing a criminal charge?
      i. The business area should have the ability to unencrypt or unmask at the DB level if an investigation is initiated
         1. TEKWave will assist in unmasking when required
4. Encryption
   a. TEKWave uses AES encryptions to store Personally Identifiable Information (PII). Encryption keys are stored within complied libraries and are not viewable or configurable by end users