

Vendor Software Assessment HIPAA Requirements Implemented

| HIPAA Standard | Y/N | If "No", any plans to be Supported? | Release Date | Comments |
|--|-----|-------------------------------------|--------------|----------|
| Access Control: <i>The protection of information or data at rest to only those users who have a business need to access the information.</i> (Indicate which of the 3 access control methods) | | | | |
| 1. User-based access | | | | |
| 2. Role-based access | | | | |
| 3. Context-based access | | | | |
| Emergency access | | | | |
| Support for permissions by patients on how their records may be used and by whom (user, group and role). | | | | |
| <i>(Optional)</i> Encryption | | | | |
| Authentication <i>The corroboration that an entity is who they claimed. Also, a communications and/or networks mechanism to irrefutably identify authorized users, programs, and processes, and to deny such unauthorized.</i> | | | | |
| Unique user identification (Required) | | | | |
| Automatic log off (Required) | | | | |
| <i>In addition, at least one of the following must be used:</i> | | | | |
| 1. Password | | | | |
| 2. Personal identification number (PIN) | | | | |
| 3. Token device for user identification | | | | |
| 4. Biometrics | | | | |
| 5. Telephone callback | | | | |
| PKI or Digital certificates | | | | |

| HIPAA Standard | Y/N | If "No", any plans to be Supported? | Release Date | Comments |
|--|-----|-------------------------------------|--------------|----------|
| Single sign-on: (Optional) Command line support of single sign-on technology. | | | | |
| Password Interval Changes: (Optional) System forces password changes at set intervals. | | | | |
| Password Rules Enforcement: (Optional) System enforces password rules. | | | | |
| Data Authentication (Data integrity) <i>A process of ensuring that protected health information has not be altered or destroyed in an unauthorized manner.</i> | | | | |
| Edit checks, check digits, digital signature | | | | |
| Other measures inherent within the software. | | | | |
| Security Audit Controls <i>A process of examining logged information to address any potential security or privacy breaches or weaknesses within the access controls or training program.</i> | | | | |
| UserID, date and time stamp | | | | |
| Unauthorized activities | | | | |
| Granularity of audit trails: Capture of keyboard strokes, mouse or other input device | | | | |
| Other measures inherent within the software. | | | | |
| Security Configuration Management <i>The management of security features and assurances through control of changes made to the system.</i> | | | | |
| 1. Documentation | | | | |
| 2. Security Testing | | | | |
| Certification <i>The process of determining whether technical security controls are implemented and meet specified criteria.</i> | | | | |

| HIPAA Standard | Y/N | If "No", any plans to be Supported? | Release Date | Comments |
|--|-----|-------------------------------------|--------------|----------|
| | | | | |
| In addition, will any of the following Privacy requirements be supported? | | | | |
| Supports flags for restrictions | | | | |
| On-line reminders for authorizations/consents | | | | |
| Amendments in patient medical records | | | | |
| Other: _____ | | | | |
| Encryption: | | | | |
| Support for both EDI and HL7 encrypted transactions | | | | |
| Support for file encryption | | | | |
| If encryption is supported, specify encryption method: _____ _____ _____ | | | | |