

## SYNCTECH™ + HEALTHCARE | APPLICABLE STANDARDS AND REGULATIONS

As a professional in the healthcare field you are probably aware how important precise time is. There are needs and requirements for accurate time in display clocks, network synchronization, documentation and medical equipment. Besides HIPAA there are many other existing and proposed procedures and applications that require accurate time.

### HIPAA

Security and Electronic Signature Standards (2002) addresses the following policies, practices, and procedures: (a few examples)

#### Security and Confidentiality Policies

Requirement for a time source behind the firewall for secure and accurate networking.

#### Audit Trails

Requirement for Legally Traceable Time to support Time Stamps, Audit Trails, File Logs, etc... that HIPAA mandates, especially as it relates to Electronic Health Records.

### CMS CONDITIONS OF PARTICIPATION FOR HOSPITALS §482.24

Defined standards and requirements for medical records, whether they are in paper or electronic format. These regulations are the foundation for maintaining a legally sound health records.

Time synchronization supports the following regulation statement:

All entries in the medical record must be timed, date, and authenticated, and a method established to identify the author. The identification may include written signatures, initials, computer key, or other code. Authentication may include signatures, written initials or computer entry.

### ASTM

Subcommittee E31.20 (Security and Privacy)  
Authentication of Computer-based Health Information

### ISO/IEC 15408-1

Security protection profile for a healthcare IT application system

### JCAHO

Provides guidelines for the appropriate authentication of medical record entries  
Standard IM 7.1.1 states that only authorized individuals may make entries in the medical record.  
Standard IM 7.8 states that every medical record entry must be dated, its author identified and, when necessary, authenticated.

### FDA 21 CFR PART 11

Section 11.10 describes measures designed to ensure the integrity of system operations and information stored in the system. Such measures include: (1) validation; (2) the ability to generate accurate and complete copies of records; (3) archival protection of records; (4) **use of computer-generated, time-stamped audit trails**; (5) use of appropriate controls over systems documentation; and (6) a determination that persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks.