Aimed at facilitating the integration of applications at the point of use, the Clinical Context Management Specification (CCOW) is an end-user-focused standard that complements HL7's traditional emphasis on data interchange and enterprise workflow.

Using a technique known as context management, the clinical user's experience is one of interacting with a single system, when in fact he or she may be using multiple, independent applications from many different systems, each via its native user interface.

By synchronizing and coordinating applications so that they automatically follow the user's context, the CCOW Standard serves as the basis for ensuring secure and consistent access to patient information from heterogeneous sources. The benefits include applications that are easier to use, increased utilization of electronically available information, and an increase in patient safety. Further, CCOW support for secure context management provides a healthcare standards basis for addressing HIPAA requirements. For example, CCOW enables the deployment of highly secure single sign-on solutions.

IMPACT

CCOW's impact on the healthcare industry is apparent. All of the major HIS vendors are now shipping or planning on shipping both Windows- and Web-based CCOW-compliant applications, while vendors in virtually every segment of the clinical healthcare market have adopted the standard as well. VHA Inc.-a nationwide network of 1,900 leading community-owned healthcare organizations and their affiliated institutions-now requires all of its new business partners to be CCOW-compliant. A growing number of healthcare organizations are also implementing context management solutions to link together diverse multi-vendor, multi-technology IT systems on an enterprise-wide basis.

HOW IT WORKS

The CCOW Work Group became a part of HL7 after starting out as an independent healthcare industry consortium. In a short time, the committee has developed and ratified five versions of the CCOW Standard. This unprecedented pace has been, in part, due to the modular component-based nature of the architecture upon which the standard is based, enabling new specifications to be developed in a complementary and add-on manner.

CCOW’s Context Management Architecture (CMA) was founded on the principle that common context can be established across applications by identifying things, such as a patient concept, or clinical encounters in a manner that different applications can nevertheless recognize.

The core architecture is comprised of three main types of components: applications; a context manager that coordinates and synchronizes applications; and mapping agents that can represent the various synonymous real-world identifiers used to identify clinical patients, users, etc. The architecture defines the roles and responsibilities for each of these components and precisely prescribes the interfaces that enable them to communicate. The architecture does not define or dictate the implementation of any of the components.

The user sets the context using any CCOW-compliant application, for example, to select a patient of interest. The application then tells the context manager that it wants to set the patient context and provides the context manager with an identifier that indicates the context subject, which, in this case, might be the medical record number for the patient of interest.

The context manager then tells the other applications that the context has been changed, and each application obtains the patient's identifier from the context manager. Each application then adjusts its internal state and data display accordingly. This all happens in real-time.

Context links may be common or secure. Any application may set or get the context data for a common link. In contrast, only site-designated applications may set and/or get the context data for a secure link. Applications, the context manager and mapping agents use digital signatures to authenticate the messages they send and receive and to ensure the integrity of the data within these messages.

The basic idea is to provide a means for the various CCOW components to trust each other, for example, to enable applications to know that they are communicating with the real context manager (as opposed to a rogue application that is pretending to be a context manager).

One of the more elegant capabilities provided by the architecture is that the use of different context subject identifiers is hidden from applications. An application only needs to know its own identifiers. A mapping agent works in conjunction with the context manager to map the identifiers used by the application that sets the context to identifiers that may be understood by other context-sharing applications. For example, one application may use a hospital-assigned medical record number to identify patients, while another application in the same institution uses clinic-assigned medical record numbers to identify the same patients.
The CCOW architecture was designed to be easily implemented within all types of healthcare applications and using a variety of technologies. Particular emphasis was given to ensuring that CCOW compliance could be easily retrofitted into existing applications. It is not necessary for an application developer to implement a context manager or mapping agents, as these components are external to the application and can be obtained from other sources.

**CCOW V1.0**

Approved by ANSI in July 1999, CCOW V1.0 defined: The overall technology-neutral context management architecture (CMA), a core set of data definitions, rules for application user interfaces, and the translation of the CMA to Microsoft’s COM/ActiveX technology. The features of 1.0 include:

- General architecture for "linking" applications: Compliant applications “tune” to the same “context subject”—such as a user, patient or encounter.
- Key context management components: The context manager coordinates applications and mapping agents, which map between the various identifiers.
- End-to-end security: Context-based security enforces subject-level access privileges such that only site-designated applications may access the values for a particular subject.
- Patient Link: This is a common subject that enables applications to tune to the same patient.
- User Link: This is a secure subject that enables applications to securely tune to the same user.
- COM Technology Specification: This is a specification of all of the details needed to implement COM-based applications and mapping agents that plug-and-play with a context manager, including all of the necessary COM interfaces.

**CCOW V1.1**

Approved by ANSI in March 2000, CCOW V1.1 added support for:

- Dependent context subjects: A dependent subject may only be set when one or more other subjects that it depends upon are also set. This ensures that the complete context, which may be comprised of multiple subjects, is always self-consistent.
- Encounter subject: This subject enables applications to tune to the same clinical encounter for a particular patient. The encounter subject is dependent upon the patient subject, so it is not possible for an application to set the encounter subject without also setting the patient subject.
- Custom subjects: A custom subject is one whose data definition has not been published as part of a ratified CCOW specification. The CCOW specification for custom subjects provides a structured way for defining the necessary data definitions and ensures that the data definition for a custom subject will not collide with those defined by other organizations or by CCOW.
- Formal conformance statements: These statements define what an application, context manager, or other type of CCOW-defined component must be capable of doing in order to claim conformance. CCOW does not address the process of validating conformance, but these conformance statements clearly establish what it means to be compliant.

**CCOW V1.2**

ANSI approved in September 2000, CCOW V1.2 added:

- Web Technologies Specification: Web technologies are quite different from the COM/ActiveX technologies defined for 1.0, but the technology mapping defined in 1.2 nevertheless enables interoperability between applications and mapping agents that employ either technology, as mediated by a context manager. Web-based applications and mapping agents send and receive URL-encoded HTTP messages to the context manager. These messages are analogous to the messages COM-based applications, mapping agents, and context managers send and receive, thereby providing the basis for interoperability between technologies.
Capability to deploy over private and public networks. The security protocols and policies defined in the CMA are used in both scenarios, but Web-based CCOW over public networks adds the use of Secure Socket Layer (SSL) as the communication substrate for all CCOW-based communication.

**CCOW 1.3**

ANSI approved in June 2001, CCOW V1.3 added the concept of annotations:

- Annotation subjects: Annotation subjects are comprised of data elements that describe something, as opposed to identify something. An annotation subject is always dependent upon an identity subject. For example, the patient subject is used for identifying the patient.

A hypothetical demographics annotation subject would contain the patient’s telephone number, address, and so on. The data for an annotation subject may only be set by annotation agent. There is an annotation agent for each annotation subject. After the context is set by an application, each available annotation agent is instructed by the context manager to add the appropriate annotation data to the context. Each site defines the data sources for its annotation agents. This ensures that applications will always see annotation data that comes from the source that is the authentic source for the data.

Two new context subjects were defined as well:

- Observation request subject: This subject enables applications to tune to the same clinical observation request, so that, for example, different applications can display the results of a particular lab test order.
- Certificate subject: This subject which is an annotation subject (see below), enables applications to tune to the same X.509 compatible digital certificate, enabling different applications to nevertheless use the same user security credentials when digitally signing and/or encrypting data on behalf of the user.

**CCOW V1.4**

CCOW 1.4 was released as an ANSI-approved standard in August 2002. One of the key features is support for multiple context sessions on the same point-of-use device. Each session may be securely "owned" by a different user, although only one context session will be active at a time. Multiple context sessions enable the CCOW standard to be even more flexible when used by caregivers who need to share devices in a kiosk-like manner. Users will be able to quickly and easily access their own sessions, and may "lock" their sessions when not in use, and then return to their sessions at a later time.

Another key feature of CCOW V1.4 is support for action subjects. An action subject enables an application to request, via the context manager, that another application perform a task on behalf of the requesting application. The request is generally issued in response to a user input or gesture. For example, certain clinical applications require that the user be authenticated in order to enter data, even though the user is already signed-on. With an authentication action, a clinical application can request that the authentication application authenticate the user.

Because this communication is context-based, the two applications do not need to know about each other and yet can nevertheless service the same user.

Other CCOW V1.4 features include: a new context manager interface, ContextFilter, that enables an application to indicate the specific context subjects about which it wants to be notified whenever the context for the subject is set, and a set of data definitions for linking applications based upon DICOM image studies.

**CCOW 1.5**

CCOW V1.5 was approved as an ANSI standard in August 2004 and reaffirmed in 2009. It is available in the bookstore area of the HL7 website: www.HL7.org.

**Approved CCOW Documents**

There are three documents based on the CCOW Standard that received ANSI approval in April 2008:

- **HL7 Clinical Context Management (CCOW) Application Protection Package, Release 1**
  This document presents the functional security requirements for a CCOW-compliant application.

- **HL7 Clinical Context Management (CCOW) Context Manager Protection Package, Release 1**
  This document presents the functional security requirements required in coordinating the component of the CCOW architecture known as the context manager.

- **HL7 Clinical Context Management (CCOW) User Authentication Protection Package, Release 1**
  This addresses the need to improve the clinical sign-on process to provide both efficiency and security. It contains functionality specific to programs that are used for authenticating computer system users and which also implement the CCOW Standard for context sharing. More specifically, this protection package describes CCOW-specific functional security requirements required for user authentication by a CCOW-compliant application.

**CONCLUSION**

The CCOW Standard continues to evolve to address an increasing set of context management capabilities. Leveraging the architectural foundation established at the onset, the standard now embraces multiple technologies, a variety of context subjects, and an increasing array of context management mechanisms. This ongoing evolution will position CCOW as a pivotal resource in the years to come for provider organizations who need an effective way to extend the utility of yesterday's legacy healthcare applications while introducing the breakthrough technologies of tomorrow.

www.HL7.org