Integration Standards

by Steve Prisoc

120 S. Riverside Plaza • Chicago, Illinois, 60606

Introduction: Standards

The essence of justice systems integration is the electronic exchange of information between disparate agency information systems. The primary obstacle to electronic information sharing between justice agencies has been, until recently, the lack of standards for electronic information exchange. Without standards, justice agencies with dissimilar systems cannot easily design or adapt their systems to share data.

Because standards for electronic justice information exchanges have recently been developed at the national level, there is no need for states or localities to develop such standards from scratch. These emerging standards can be adopted to facilitate electronic information sharing between disparate justice systems at all levels—federal, state and local—so it is only necessary to actually develop standards for those very limited, unique exchanges that apply solely to a particular jurisdiction, locality or state.

What jurisdictions, states and localities must do, however, is precisely map all data elements that are exchanged as a part of normal workflow between their justice agencies. Once these data elements are mapped, appropriate standards can be applied to mapped elements in order to allow for seamless agency-to-agency electronic information transfers in a standards-based justice environment. Not all data elements in use in a particular area need to be mapped. In many cases, only elements that pertain to an offender's status, court events and criminal history need to be mapped. Regardless, all of the elements stored in various agency systems don't need to be mapped; only those that are actually exchanged must be mapped.

Although universal sharing standards aren't absolutely necessary to electronically exchange information, most electronic data exchanges that have been developed without standards are needlessly cumbersome. Exchanges of this type usually require expensive and time-consuming development of custom data exchange interfaces. These custom interfaces allow for the translation of data elements from one system to another; but the interfaces, once developed, cannot easily be reused when creating an additional interface with other entities. As a result, justice agencies that wish to expand their data sharing efforts to include multiple agencies must frequently create a new custom interface for each discrete agency-to-agency data exchange attempted. The cumulative result of this type of custom interface development is a tangled *ad hoc* data exchange architecture that is undependable and difficult to maintain. Moreover, because of high development costs, this type of data exchange architecture limits the overall value of data exchanges between justice agencies, and perhaps more importantly, limits the use of electronic data exchanges to the few agencies that can afford the required custom programming.

While adoption of universal standards for information exchange is desirable, because of the difficulties of forcing many independent elected and appointed officials to strictly adhere to a common standard, it many not be possible to impose mandatory rules and regulations pertaining to information exchanges between all independent justice agencies in a particular jurisdiction. It should, however, be possible to provide standards that can be adhered to *voluntarily* by agencies wishing to exchange data. These standards should not be created for the purpose of regulating justice agencies; rather, they should provide agencies with the tools they need to develop systems that can seamlessly share information with partner justice agencies. Without universally applicable standards, information sharing must be negotiated on an agency-by-agency basis and each information-sharing interface must be independently programmed. This is obviously inefficient and costly.

Standards, Regulations, & XML

The International Standards Organization (ISO) describes the difference between standards and regulations as follows:

> **Standard** – A document approved by a recognized body, that provides for common and repeated use, rules, guidelines, or characteristics for products, processes or services for which *compliance is not mandatory*.
>
> **Regulation** – A document that describes product, process or service characteristics, including the applicable administrative provisions, with which *compliance is mandatory*.

Justice agencies that voluntarily adopt data exchange standards will more easily be able to exchange justice information among themselves, but it is not likely that all agencies will adopt data exchange standards immediately. However, once data exchange standards gain wide acceptance, thus increasing the number of potential exchange partners, agencies will adopt these standards in increasing numbers.

In addition to *standards* to facilitate information exchange, there is a need for *regulations* that will mandate minimum levels of security. Also needed are regulations to ensure consistent telecommunications protocols for transferring data between agencies. Many regulations of this nature are currently in effect, such as those used to facilitate the transfer of arrest and disposition information between local agencies and central criminal history repositories. Other examples include regulations that dictate proper methods for transmitting fingerprint information from local agencies to the state agencies that classify fingerprints and identify offenders. Also important are data security and user training regulations that must be met before users gain access to state and national criminal history systems.

As noted earlier, much work continues to be accomplished at the national level to develop standards to facilitate the sharing of justice information between authorized justice entities. Most of this work has centered on the creation of XML (eXtensible Markup Language) conventions that when implemented allow data to be seamlessly transferred and simultaneously translated as they are passed from one justice agency to another. There are several groups now operating that have already developed working models for such standards and are now in the process of refining and reconciling these standards into a single, uniform justice XML definition that can be used by justice agencies throughout the world.

XML is widely touted as a technology that can facilitate the seamless exchange and simultaneous translation of data between disparate systems. XML is not the only method available for data exchange between systems, but it is by far the most accepted. At present, all major vendors of database software—IBM, Oracle, Microsoft and Sybase—have invested significantly in making their software fully XML compliant.

Organizations at the national level that are making significant progress in this area of XML exchange standards include SEARCH, the National Association of State Chief Information Officers (NASCIO), the U.S. Department of Justice, the Industry Working Group (IWG), GLOBAL, the National Center for State Courts (NCSC), and the Justice Integrated Systems Professionals (JISP). All of these groups are working toward the common goal of creating a uniform set of XML data description tags that will facilitate meaningful data transfers between dissimilar systems. Several states, including Illinois, are in the process of reviewing and commenting on the emerging XML data standards.

In Illinois work is now being performed by workgroups operating under the auspices of the Illinois Integrated Justice Information System (IIJIS) Board. These groups are working to identify and catalog justice information exchange points and match associated data elements to emerging justice XML data description tags. The ultimate goal is to apply agreed-upon XML data description tags to the justice data elements most frequently transferred from one agency to another during the course of the justice process. Once documents that result from these efforts are released to justice agencies, they will provide much-needed data exchange standards to the Illinois justice community. The ongoing results of this work are posted at www.icjia.state.il.us/iijis.

Once promulgated, these standards documents will not remain static for long. It is vital that justice exchange standards be constantly reevaluated for appropriateness and relevance to the evolving needs of the justice system. This means that local groups of individual stakeholders must continually evaluate the suitability of emerging national standards and provide feedback to groups at the national level responsible for maintaining these standards.

Functional Standards for Justice Systems Development: Reducing the Need for Data Exchange Standards

Some states have developed or are now developing information systems that can be used statewide by particular segments of the justice system. For example, Wisconsin has developed a standard prosecution system, PROTECT, that can be used by all District Attorney's Offices in the state; its rollout and adoption by all counties in Wisconsin is a major part of that state's integration effort. By establishing a common *functional* system standard with common data definitions, data exchanges between the county prosecutors using the system will be much easier. It would be reasonable to assume that future systems developed for other justice agencies in Wisconsin would also use the same functional standards when applicable.

This type of direct information sharing shouldn't be confused with exchanges enabled by adopting standards that will allow for the pushing and pulling of translated information between agencies using disparate systems on an as-needed basis. The use of a common system greatly reduces the need for data exchange standards since all data stored by that system will be in the same format and all data elements will be uniform across agency boundaries. Such shared systems do, however, require that regulations be developed to ensure data quality, timeliness and accuracy.

In addition to the development of shared systems, there are efforts among some states and at the national level—particularly among court agencies—to define common functional system specifications that will create a level of data consistency. Data consistency can also reduce the need for data exchange standards among the agencies that comply with the common system specifications. An example of such an effort might be the adoption of a uniform specification—a specification for common data elements and allowable data values—for court system data within a state or jurisdiction. While such a uniform specification will make information sharing between participating court agencies less difficult, data exchange standards will still be needed if the courts intend to exchange information with non-court agencies—law enforcement, prosecution, etc.

Communications and Data Security

The data communications security field is quickly evolving. Justice systems technologists must continually monitor new security threats and become skilled with the new technologies developed to combat the threats. Because of the nature of data communications, it is now possible—even likely—for data to pass through multiple networks before it finally reaches its intended user. It is therefore important to develop regulations specifying the minimum level of technical security for all networks participating in a state or local information sharing initiative. It is also important that all communications networks be monitored and periodically audited for compliance with security regulations. There is a significant amount of work taking place at the national level that will regulate data communications security of any communication involving justice information—particularly criminal histories—and local practitioners should become actively involved in these efforts.

Illinois has a relatively rich data communications environment. Common carriers have installed robust data communications trunks throughout most of the state, and the State of Illinois provides Wide Area Network (WAN) Services to most of the state through two programs: the Central Management Services Frame Relay Network and the Illinois Century Network. Both of these networks can be used by justice agencies to make data connections to other justice agencies. Cook County has also implemented a WAN and the Illinois Criminal Justice Information Authority (ICJIA) operates a WAN that serves its law enforcement systems users. There is currently no need to develop communications protocol standards in Illinois, since all of the aforementioned providers support the TCP/IP standard (Transmission Control Protocol/Internet Protocol), so until TCP/IP is superceded by newer technologies there will be no need to examine that *de facto* standard.

The Internet offers opportunities for relatively inexpensive data communications between justice agencies. The state of Kansas is now utilizing the Internet transfer of justice information, including criminal history information; however, Kansas has implemented state-of-the-art security including a virtual private network (VPN). The ICJIA also supports a VPN to provide secure communications for users of the InfoNet, a system that provides case management to 120 victim service sites throughout Illinois. The Infonet, by utilizing the public Internet as its communications backbone, offers opportunities for making justice information available to users in areas of the state not well served by common carriers. Additionally, use of the Internet offers significant opportunities for cost savings. On the downside, use of the Internet significantly raises concerns regarding data security. The ICJIA has dealt with security by using the VPN, which enables communications to be encrypted. The VPN also requires the use of token based authentication and individual user passwords. Also, no personal identifiers are transmitted over the Internet, thus ensuring that anyone gaining unauthorized access would not be able to link case information to a particular person, virtually eliminating any risk of damage through unauthorized access.

Though the Internet is becoming more accepted as a standard vehicle for transmitting secure data, security standards and regulations must be developed and agreed upon before justice related data can be transmitted on a large scale. One effort now underway in Illinois that may provide a basis upon which to build communications security regulations is the digital signature project being spearheaded by the Illinois Technology Office (ITO). Digital signature technologies provide complete end-to-end security between the certificate holder and the provider agency, and will soon be available to agencies wishing to share justice information in this manner. The ITO has selected a common digital signature certificate authority and is providing certificates to potential users who want to communicate electronically with state agencies.

Putting Standards to Work: Schemes for Implementation

Some states have created one-stop criminal information data warehouses and/or information portals. In the case of data warehouses, information is gathered from contributing agencies and deposited in the data warehouse; the data is then structured so that individual users—based on their level of authorization—can access needed information in a variety of ways. If information exchange standards have not been pre-defined, this method requires development of rigorous conversion and cleansing routines in order for data to be consolidated from several sources (which is the most difficult part of implementing a data warehouse). Information exchange standards can facilitate the gathering of information for a data warehouse by eliminating the need to convert each agency's data at the receiving end, or having to impose strict electronic data report regulations on the reporting agencies. If data exchange standards have already been developed and/or adopted by the agencies that feed the data warehouse, it becomes much easier to populate a data warehouse with relatively clean data.

A portal, on the other hand, is a single interface through which authorized users can access a variety of offender information from a variety of agency sources. An analogy could be made here to a shopping mall that houses a number of individual shops, but each store maintains its own inventory, cash registers and security. The customer can access all shops by visiting the mall but does business directly with each shop owner. The data warehouse model is more comparable to a department store where purchases from any department can be paid for at any cash register. Kansas, Nebraska, and Pennsylvania now have data warehouses and Internet portals in place that provide justice information to various authorized users. Portals make it easy for users to access a variety of agency systems through one terminal interface, but don't really address the information-sharing problem. Portals, however, are a good first step in the integration process.

Two notable examples of criminal justice data warehouses are Los Angeles County's CHRS system and the Chicago Police Department's CLEAR system; both are criminal history repositories, but they differ from typical criminal history repositories in that their data warehousing technologies allow much greater flexibility in querying databases. These queries, which can be defined by users, go far beyond the usual restrictive, pre-defined methods for accessing criminal history data.

Justice information portals have been created by states such as Nebraska and Pennsylvania. These portals allow users to access justice information through a Web browser (but typically not over the public Internet). It is important to note, however, that this multiple-source information is not combined into one common data store, but rather each agency's information is made available through a single interface—sometimes even on a single screen. The actual data is still completely controlled and formatted by the source agency, and the data isn't aggregated into a common data warehouse. The portal simply provides a single interface through which authorized users can access data from a variety of agency systems.

Even though data warehouses and portals accomplish similar ends, ultimately, the data warehouse has the ability to format and deliver customized information to decision makers more efficiently and effectively than the portal. The data warehouse, however, will typically require more preparation and planning since information gathered from several sources will need to be merged, cleansed and organized. While not as flexible in terms of delivering tailored information to individuals, the portal approach can be implemented more quickly and can therefore serve as an early “quick win” for an integration initiative. The portal approach could also be considered a logical first step toward a data warehouse. The portal doesn’t require data exchange standards because there is no data being exchanged; however, the portal will require agreed upon security protocols and standard user authentication processes so that users won’t have to sign on to each individual agency taking part in the portal, which would defeat its purpose.

There is a third model that has not yet been effectively implemented by any state. In this model, data is aggregated, real time, as needed, from various agency systems at the time the user requests it. This model requires careful adherence to data sharing standards and also requires high data quality levels—data quality levels that most jurisdictions don’t presently enjoy.

Conclusion

It is important for justice policy makers to understand the nature of information sharing and what standards can do to facilitate such sharing. It is also important that they understand data communications standards and regulations that influence the security of the information and the speed with which information can be transferred from one agency to another. Additionally, it is especially important for policymakers to know that the biggest problem facing integrators today is the fact that justice information systems vary enormously, and at present, information cannot be easily moved from one system to another. With the adoption and application of standards for information sharing, this problem can be surmounted; without such standards, it is unlikely that electronic sharing of information between systems on a large scale will be achieved.