Electronic Disease Surveillance and Reporting: the *e*Report System

William P. Malloy and Latanya Sweeney
School of Computer Science and Heinz School of Public Policy
Carnegie Mellon University
Pittsburgh, Pennsylvania

The availability of inexpensive computers and the popularity of the World Wide Web ("Web") have encouraged the development of inexpensive, readily available software that enable secure financial transactions over the Web. This same "e-commerce" technology consisting of database-backed web sites, web-based forms, secure communications and digital signatures can be used for securely reporting and sharing sensitive information about communicable diseases and outbreaks to public health entities throughout the United States.

Identifying outbreaks and controlling the spread of communicable diseases are goals central to public health entities throughout the United States. However, in many places, most reporting is done manually by telephone, fax or mail. Compliance is sometimes spotted and can suffer from lengthy delays. The most common problem encountered centers on legacy systems. Information that could be automatically reported resides in one system, but communicating that information to another system is often technically difficult because of differences in vocabularies, data storage formats and electronic communication standards and capabilities. Web technology is ubiquitous.

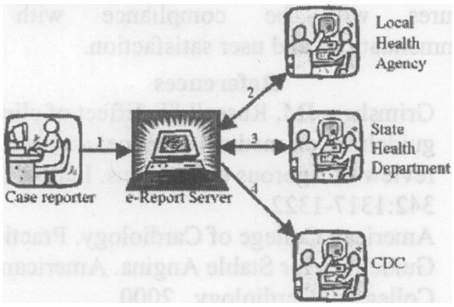

Figure 1 Information flow and controls

The *e*Report System allows authorized agents to report a case over the Web, manually through configurable, self-checking forms or automatically using a prescribed protocol. Security and privacy are of utmost importance. Authorizations within the *e*Report System release data at varying levels of anonymity, enforcing a strict need-to-know policy. The *e*Report system utilizes authentication, audit trails, password and session management, encryption, and disclosure controls. Figure 1 shows the flow of information in *e*Report, respecting traditional authorizations from local agencies to state agencies, and then to the Centers for Disease Control and Prevention.

The *e*Report prototype exploits the latest technology, as shown in the system overview in Figure 2. When an HTTP session begins, the user's browser displays a JSP login page. The security manager either validates or denies access to a navigational page. If access is provided, a user can report a case, edit an existing case report, or view summary information, as the user's credentials warrant. The security manager can further restrict shared content based on geography and privacy constraints. Information is stored in a relational database with servlet connections. The result is a robust, secure reporting environment.

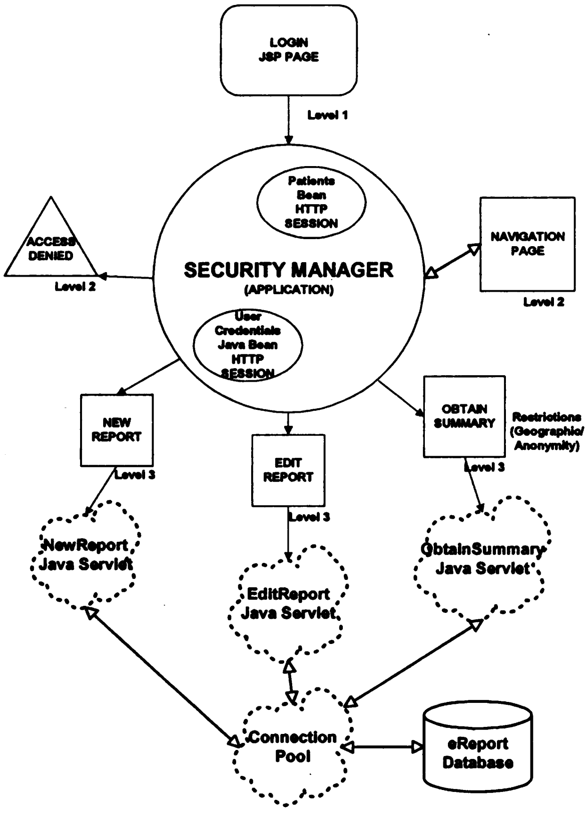

Figure 2 System overview of *e*Report

Given the economics, speed, reliability and security of *e*Report, it serves as a model to inform and improve public health surveillance effectiveness and reporting compliance and timeliness.