Multi-Tier Role Based Access for Secure and Flexible Syndromic Surveillance

Meichun Li, MSIS, Amy Ising, MSIS, Raghu Havaldar, MS, Anna Waller, ScD

Emergency Medicine, School of Medicine, University of North Carolina, Chapel Hill, NC

OBJECTIVE

This paper describes the role-based access used in the North Carolina Disease Event Tracking and Epidemiologic Collection Tool (NC DETECT) Web portal for early event detection and timely public health surveillance.

BACKGROUND

NC DETECT receives data on at least a daily basis from five data sources: emergency departments (ED), the statewide poison center (CPC), the statewide EMS data collection system, a regional wildlife center and laboratories from the NC State College of Veterinary Medicine. A Web portal is available to users at state, regional and local levels and provides syndromic surveillance reports as well as reports for broader public health surveillance such as injury, occupational health, and post-disaster. The current portal is built on access controls initially designed in 2002 for hospital-based users only. The role-based access was modified slightly in 2004 to accommodate public health epidemiologists (PHEs) at the local, regional and state levels who wanted county-based report access. The design used, however, was shortsighted and limited. For example, the controls cannot accommodate certain users' access to non-ED data sources as well as the ability to retrieve protected health information (PHI) via the portal when needed for investigation. These evolving user needs have led to a full system redesign with a much more robust security model.

METHODS

We have used an iterative, user-centered design approach with the redesign. Several meetings have been held since the fall of 2005 to discus user access needs, including what is needed for effective surveillance as well as what are the state legislated restrictions that may affect data access. The challenge is to control data access with multiple tiers: data source, geography, aggregate data, line listing data, PHI, and annotation privileges - functionality in the new system allowing authorized users to document signals and keep track of signal investigations. The revised user role matrix was finalized in June 2006 and is now being incorporated in the new system using database driven controls with a Java front-end.

RESULTS

Role-based access revisions have been driven primarily by state mandates governing public health investigation. There are laws explicitly granting data access to ED data for certain public health threats [1], but access to non-ED data sources is more nebulous. As a result, users explicitly involved in communicable disease or bioterrorism surveillance have more data access privileges than users at the same levels in occupational health or injury surveillance. For example, state level communicable disease epidemiologists (GCDC) are able to access aggregate data, line listing, PHI and annotation of all data sources, while non-GCDC branch users have no access to CPC line listing and PHI. Regional epidemiologists are also granted access to aggregate, line listing, PHI and annotation for all data sources, but are limited to the counties and hospitals in their own region. Hospital-based PHEs have access privileges to aggregate, line listing, PHI and annotation for ED data of their affiliated hospital(s), and can view aggregate data of all data (ED and non-ED) sources. Specific data source users can access line listing and aggregate for their respective data source only. Public health users at all levels who are not tasked with threat investigations are limited to aggregate data.

The role-based security model developed for the new system is defined based on geography, data source, the right to access aggregate data, line listing data, PHI, and annotations. While most of the user roles can be pre-defined, the system is flexible enough to allow for customized data access, and, thus, it is possible to meet the needs of all potential NC DETECT users.

Access to PHI is strictly controlled. PHI is encrypted in the database and only authorized users have access to it through the SSL-enabled web portal. The window that displays the PHI closes automatically after one minute, and all access to PHI is logged in detail.

CONCLUSIONS

With revised data access controls, NC DETECT 4.0 provides users at all levels with secure and tailored access to syndromic, injury, post-disaster, occupational health and other types of surveillance reports. Role-based access designs must be flexible enough to accommodate changing user needs as well as state and federal privacy and security regulations.

REFERENCES

[1] North Carolina General Statute 130A-480. http://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_130A.html. Accessed June 30, 2006.