Emerging Health Threats Journal 2011, **4**:s79. **doi:** 10.3134/ehtj.10.079

www.eht-journal.org

ABSTRACT

Securing protected health information in NC DETECT

DM Falls, M Li, and A Waller

Carolina Center for Health Informatics, Department of Emergency Medicine, UNC, Chapel Hill, NC, USA
E-mail: dfalls@med.unc.edu

Objective

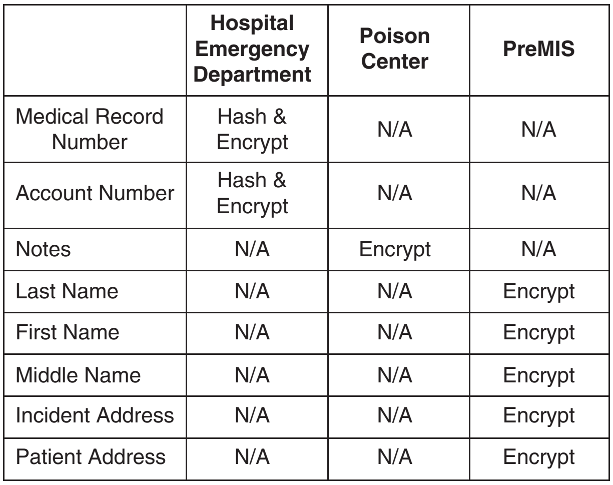
This paper describes how the North Carolina Disease Event Tracking and Epidemiologic Collection Tool (NC DETECT) utilizes various methods of encryption and access control to protect sensitive patient data during both integration and reporting.

Introduction

NC DETECT receives daily data files from emergency departments (ED), the statewide EMS data collection system, the statewide poison center, and veterinary laboratory test results. Included in these data are elements, which may contain Protected Health Information (PHI). It is the responsibility of NC DETECT to ensure that security of these data is managed during their entire life cycle, including receiving, loading, cleaning, storage, managing, reporting, user access, archiving, and destruction. A web interface is provided for users at state, regional and local levels to access syndromic surveillance reports, as well as reports for broader public health surveillance such as injury, occupational health, and disaster management.

Methods

Data files are downloaded via the internet using both Secure File Transfer Protocol (SFTP) and Secure Hyper Text Transfer Protocol (HTTPS). An off-the-shelf Extraction, Transformation and Loading (ETL) tool, capable of receiving data from any of nearly 200 data types including ASCII, HL7 and XML, allows for easy database loading and data encryption. A combination of secure hash algorithm (SHA-1) and triple DES encryption algorithm are used to secure PHI upon database loading. Role based access with multiple tiers controls, data source, geography, aggregate data, line listing data, PHI, and annotation privileges, functionality which allows authorized users to document signals and keep track of signal investigations.



	Hospital Emergency Department	Poison Center	PreMIS
Medical Record Number	Hash & Encrypt	N/A	N/A
Account Number	Hash & Encrypt	N/A	N/A
Notes	N/A	Encrypt	N/A
Last Name	N/A	N/A	Encrypt
First Name	N/A	N/A	Encrypt
Middle Name	N/A	N/A	Encrypt
Incident Address	N/A	N/A	Encrypt
Patient Address	N/A	N/A	Encrypt

Figure 1 Security methods per data source/data element.

Data files are retained for 14 days in a location secured using Windows Encrypted File System (EFS).

Results

NC DETECT currently receives data from 120 hospital-based emergency departments, 100 EMS systems, and the state poison control center. Eight various data elements are either encrypted, hashed or both (Figure 1).

There are 356 active web interface users; 276 are authorized to access limited PHI based on professional role and geographical location.

Conclusion

PHI must be secured for both storage and transportation. NC DETECT's data processing system provides the functionality to meet HIPAA standards for data storage encryption[1] and our Role Based Web Interface provides protection of data being transmitted across the internet.[2] 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 public health 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.

Acknowledgements

Funding for NC DETECT is provided by the North Carolina Division of Public Health. This paper was presented as a poster at the 2010 International Society for Disease Surveillance Conference, held in Park City, UT, USA on 1–2 December 2010.

References

1 45 CFR Part 142, § 142.308 (c). 'Technical security services to guard data integrity, confidentiality and availability.'
2 45 CFR Part 142, § 142.308 (d). 'Technical security mechanisms.'