Personal identity verification for regional emergency workers

Alexander McLeod Jr.*

Accounting & Information Systems Department
College of Business Administration
University of Nevada
Reno, NV 89557, USA
E-mail: amcleod@unr.edu
*Corresponding author

Eric Epley

Southwest Texas Regional Advisory Council for Trauma
7500 Highway 90 West # 200
San Antonio, Texas 78227, USA
E-mail: eric@strac.org

Rasa Silenas

Texas A&M University System Health Science Center
Office of Homeland Security
College Station, Texas 77840, USA
E-mail: rasa@silenas.net

Abstract: South Central Texas emergency planners have organised a regional Personal Identity Verification (PIV) project for hospital and emergency workers. This paper describes the development and administrative challenges in designing and implementing an electronic PIV system across multiple organisations in a 22-county region.

Keywords: Personal Identity Verification; PIV; emergency worker identification; regional ID system; regional identity verification; e-healthcare.

Reference to this paper should be made as follows: McLeod, A.J., Jr., Epley, E. and Silenas, R. (2008) 'Personal identity verification for regional emergency workers', *Int. J. Electronic Healthcare*, Vol. 4, No. 2, pp.153–165.

Biographical notes: Alexander McLeod Jr. is an Assistant Professor in the Accounting and Information Systems Department at the University of Nevada, USA. His research interests include organisational performance, information systems security, emergency response systems and healthcare information systems. He has published in *Communications of the AIS* and the *International Journal of Electronic Healthcare*.

Eric Epley is the Executive Director of the Southwest Texas Regional Advisory Council for Trauma for San Antonio and South Texas, USA. He led the organisation through several initiatives, including a regional Emergency

Medical Service (EMS) electronic charting project, an EMS/trauma registry and a medical operations center for disaster/terrorism response. He is the chair of the EMS/Hospital Disaster Group.

Rasa Silenas, M.D., F.A.C.S., is an Associate Research Scientist and Medical Director of the Texas A&M University Health Science Center, the Office of Homeland Security. She has published research in the areas of hospital bioterrorism preparedness, public health and syndromic surveillance, public health nursing and regional and governmental disaster management and response.

1 Introduction

Managing personnel identification and access control for workers who are not their employees is a significant security issue for hospitals, and carrying a plethora of identification badges is a nuisance for healthcare and emergency personnel who work in multiple hospitals (Ahn and Lam, 2005). This paper describes one region's electronic healthcare solution.

After the terrorist attacks of September 11, 2001, leaders from hospitals, Emergency Medical Services (EMS), and Public Health and Emergency Management in the greater San Antonio region organised a voluntary committee to improve regional preparedness following national hospital accreditation recommendations (Autrey and Moss, 2006). One of the workgroups under this committee is the EMS/Hospital Disaster Group (EHDG), which focused on hospital and pre-hospital aspects of medical disaster response. The EHDG was a technologically capable volunteer group with no formal authority. EHDG aligned itself with the Southwest Texas Regional Advisory Council for Trauma (STRAC), which has a state legislative mandate to organise EMS and trauma system response on a regional level, as its standing disaster committee. Additionally, the region's hospital leadership designated EHDG as the planning group for Health Resources and Services Administration (HRSA) Bioterrorism funds, allowing federal funding to support the preparedness plans of EHDG. By becoming a standing committee of STRAC and acquiring authority from the regional hospital leadership, EHDG and its workgroups became empowered to function as a regional technological resource to solve problems. This type of leadership was badly needed in order to address regional preparedness problems (Hanfling *et al*., 2004).

One of the first problems that EHDG identified was that the hospitals and Fire/EMS agencies within the 22-county STRAC region did not have a uniform method for identifying physicians and Fire/EMS personnel and disaster volunteer medical workers. This created three primary concerns for regional emergency preparedness:

1 difficulty securing hospitals and other facilities

2 inability to identify and authenticate affiliated medical professionals

3 lack of adequate identification and tracking of personnel at routine Fire Department and EMS responses as well as disaster incidents.

These types of issues are not unique to one hospital or service and require resolution throughout the area (Cieslak, 2003). Because of the size of the region (22 counties, 26 000 square miles) no single personnel accountability system existed. The large municipal fire department operated a sophisticated incident command system, but lacked the ability to identify medical professionals. While they had purchased software to manage incident command, this system had not been implemented leaving identification to on scene tracking to manual methods.

2 Process

To address these problems, EHDG tasked its Hospital Security workgroup to develop the concept of a uniform identification (ID) badge for the region. The Bexar County Medical Society (BCMS) was approached as a possible partner to address a number of its needs, including assisting hospitals' compliance with the requirement of the Joint Commission for Accreditation of Healthcare Organizations (JCAHO) for hospital personnel and physicians to wear identification. The Bexar County Medical Society embraced the project. Other early supporters included all STRAC EMS agencies, the San Antonio Fire Department (SAFD), the Bexar County Fire Marshal's Office (BCFMO) and the Alamo Area Fire Chiefs Association. Approximately $150,000 was allocated to the project in the 2003 fiscal year.

3 Initial steps

Risk assessment: The EHDG requested briefings from Emergency Management personnel, the Federal Bureau of Investigation (FBI), and others. Inadequate hospital and disaster site security was high among the concerns identified in these risk discussions, specifically the inability to:

- rapidly and effectively lock down a facility, while remaining functional for patient care
- easily identify the various non-hospital employees that routinely enter and exit hospitals (Physicians, Fire/EMS personnel, and during disasters, volunteer medical workers)
- track non-traditional personnel at a disaster incident (self-presenting physicians, disaster medical volunteers, Fire/EMS personnel from other jurisdictions, *etc*.). Review of local and other disaster after-action reports reveals that such personnel have created significant problems, ranging from non-licensed personnel practicing medicine to the inability to know who was left in a particular area when the location was evacuated
- use the Personnel Accountability Reporting (PAR) system for all personnel at an incident site
- instantly know the certification level of other medical personnel and the current level at which their agencies' local policies allow them to practice.

The threat of terrorism has amplified these concerns, especially the ability to rapidly secure a hospital and remain in a lock-down mode for an extended time. Since January 2003, the Department of Homeland Security (DHS) has put the nation at Threat Level Orange twice, for weeks or months at a time. Security alerts have referenced the potential for terrorists to obtain Fire/EMS uniforms and ambulances to gain access to secure areas. The possibility for physician impersonation exists as well, with possible penetration into hospitals, including sensitive hospital areas such as Intensive Care Units or pharmacies. Hospitals have not been able to implement higher security measures without significant hindrances to daily operations.

4 Access control assessment

In order to evaluate the current state, EHDG personnel performed a risk assessment of hospital access control systems in the area. Members of the committee visited each hospital and discussed access control with members of internal security. Each hospital was a member of STRAC and had previously committed to participation as part of their JCAHO certification process. JCAHO had specified that emergency departments should assess and plan for extended lockdowns due to terror threats. Lockdown included access control. They found four main technologies in use, from multiple vendors:

1 varieties of magnetic stripes on the card, which require a swipe of the card through a card reader, similar to a credit card swipe

2 proximity Radio Frequency Identification (RFID) cards or other devices that emit a small signal that wirelessly connects the card to the reader

3 one-dimensional bar codes, which require a bar code scanner, similar to the type used at the checkout counter of the grocery store

4 keypads that require personnel to remember a specific numerical code to enter the door. Most ED keypads in the city were programmed to variations of a single, simple code, creating vulnerability.

Some facilities used a mixture of these technologies.

5 Initial goals and assumptions

The uniform ID badge had to meet a complex set of requirement from badge wearers, hospitals, Fire/EMS and Emergency Management agencies. Physicians and Fire/EMS personnel, as prospective badge holders, had similar desires. Their ideal ID badge would:

- allow entry to areas where the cardholder has approved access
- restrict movement into areas where the cardholder does not have approved access
- provide easy visual identification, at least with picture, first/last name, clinical certification/license, specialty/rank and home agency if applicable

- provide additional data directly from the card to a reading device (such as a laptop or handheld card reader) that would give incident command or security personnel additional details not normally desired on the visible portion of the card. This might include additional qualifications and other information, such as medical history, blood type, or smallpox vaccination status
- have a simple and quick process for requesting, obtaining and replacing the card while maintaining the ability to verify the badge-holder's credentials
- ensure security of the ID badges and validate the data associated with them
- reduce the number of badges and parking cards an individual needs to carry.

Hospital, Fire/EMS and Emergency Management agency desires, as badge system users, included the following capabilities:

- Visual/manual identification of personnel with an easily recognised ID badge that is consistently worn.
- Ability to scan the ID badge for additional data about the badge-holder, such as clinical skills, specialty knowledge, and medical information such as immunisation status.
- Ability to implement restrictive hospital access control during heightened security without a significant impact on daily operations.
- Hospital compliance with JCAHO requirements with respect to physician identification, while also providing an easy method for physicians to comply with these requirements.
- Ability for Fire/EMS and Emergency Management agencies to track and maintain accountability for personnel on an emergency scene to ensure their safety when safety conditions deteriorate.
- Tracking, with time stamp information, of badge-holders who have entered specific areas of a hospital or other access-controlled facility.
- Ability to track personnel who were possibly exposed to a contagious/infectious agent or hazardous substance.
- Ability to immediately lock out an individual whose employment with an agency or affiliation with a hospital is terminated.

In the initial stages, badging was to begin with practitioners who regularly work at hospitals but who were not hospital employees: physicians and EMS. Hospitals needed to agree to the concept of uniform badging for these groups and to modify their access control systems to accommodate input from the uniform ID system allowing the uniform ID card to serve as the card-holder's method for entering the building or authorised areas such as parking facilities. The hospitals were to retain full control of who has permission to enter specific areas of their facilities. Because many of the hospitals had similar access control, no existing card reader technology was excluded. It was thought that by using existing technology and focusing on the lowest common denominator, hospital buy-in would be maximised. SAFD would participate by badging the majority of area EMS personnel.

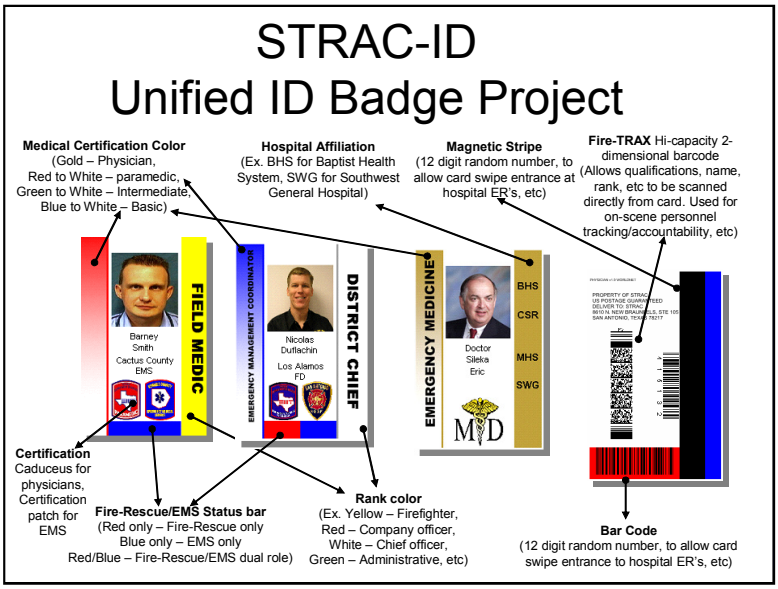
6 Badge design

A mixture of the technologies was selected to accommodate all of the above needs. The badge is a 3.3 inch tall x 2.1 inch wide Polyvinyl Chloride (PVC) card that has information printed on both sides. The visual layout of the front of the badge was based on a design in use by the Austin/Travis County EMS System and includes badge-holder demographic information such as a digital photograph, first and last name, specialty and agency affiliation. Collaboration between the participating agencies allowed the creation of a standardised color scheme which, when printed on the badge, indicates medical certification, title/rank and access type. Images of the agency's logo and medical certification patch further assist with identification of the badge-holders credentials. The various populations (physician versus Fire/EMS) have different colored layouts on the front of the badge but include the same basic information for visual identification.

The back of the badge contains an industry standard three track magnetic stripe that is encoded during production to contain access control information. The addition of a PDF-417 2-D bar code allowed interoperability with FireTrax, a proprietary system from Salamander Technologies, which facilitates personnel accountability at emergency scenes. A one-dimensional bar code (along with the magnetic stripe) is used to interface with the access control systems and achieved compatibility across multiple legacy systems already in daily use at participating facilities. The current version of the badge does not implement the use of RFID or proximity due to limited local demand and cost factors, however, the uniform ID system can accommodate these technologies when their use becomes more widespread. The addition of a second one-dimensional bar code provided agencies with an option to integrate an employee ID number into the badge for equipment tracking or timekeeping applications.

Future versions of the badge, designated v2 badges, will incorporate smart badge technology with on-chip biometric capabilities to ensure authenticity and will comply with FIPS201 requirements. The current badge used the two dimensional encrypted PDF 417 code for authentication. The unified emergency worker id badge is shown in Figure 1.

Figure 1 Badge design (see online version for colours)



7 ID system design

Once the overall look and functionality of the badge was formalised, the next step was to design and implement a system in which the badges could be easily created, managed and produced. BCMS collaborated with a local technology firm, World Net, to create the system, because this company offered knowledge and experience in both internet application development and emergency response.

The application was designed to provide a user-friendly interface to multiple concurrent users located throughout the 22 county region. The basic functionality included the ability to create, edit, review, and print badges along with extensive reporting capability. Because each agency possesses a unique set of access control and identification requirements, a matrix of access levels was designed to allow users to perform tasks commensurate with the role assigned by each agency. Each agency governed permissions and controlled ID cards for their employees. In order to avoid the unauthorised production of badges on the system, specific permission is granted to agencies with badge printers. Each agency issued badges via its security personnel and printers were placed in secure locations. On the back-end, a database was employed to manage the data. The system design included the means necessary to communicate with the access control system at each hospital in order to distribute access information for the badge-holders.

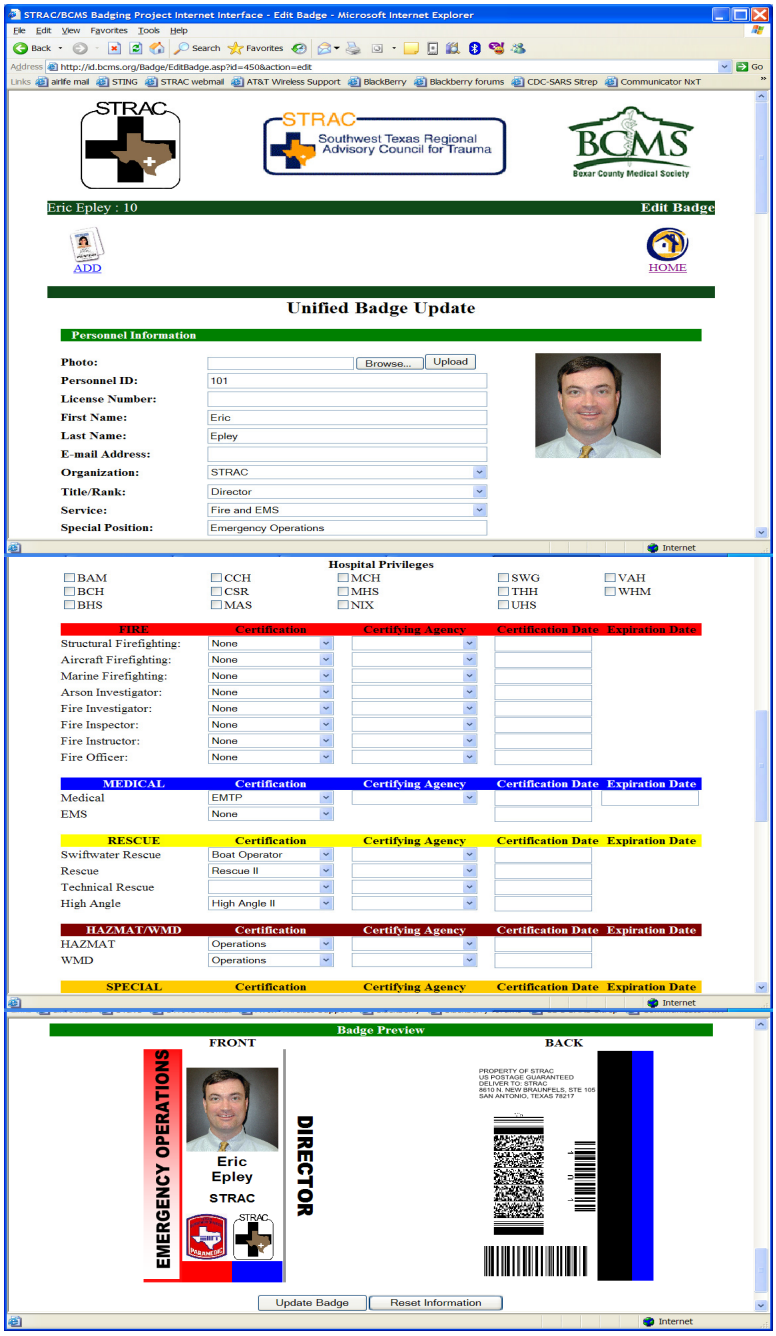
The enrollment process uses a Secure Socket Layer (SSL) encrypted Web-based application housed on a central server. Each agency must authenticate prior to using its printer. Authorised and authenticated personnel from each agency input badge-holder information into a database. A variety of fields meet the needs of all users, however each agency is only able to access data fields specific to their agency or group. Each agency authorised on the system enters basic identification information, rank, clinical licensure and certifications, along with other fields, both mandatory and optional. This interface and the current database fields are shown in Figure 2.

Hospital administration of the system includes authorising physicians access to hospital facilities by ‘affiliating’ individual badge-holders in the database, authorising badges to be printed and/or activated, as well as printing and issuing the badge. Authorised staff members at each hospital may log onto the server and affiliate badge-holders with the specific hospital but are unable to affiliate or disaffiliate badge-holders with other hospitals. The access control system at each hospital communicates with the uniform badge server at least once every 24 h to retrieve the unique access ID numbers of affiliated badge-holders. The hospital’s access control system then grants the affiliated badge-holders access to an area or group of areas as determined by the individual hospital. For instance, many hospitals granted access into parking facilities in addition to the ED doors to entice badge-holders to always carry the card.

Since the hospital’s access control system determines what areas the badge-holder may enter, individual hospitals may allow access to specific areas within the facility. Under extreme conditions, many of the hospitals anticipate limiting electronic access to the building, opting for a single portal with security personnel verifying the picture to the cardholder. However, conceivably, as the event moves into recovery phase, an agency may allow temporary access to allow physicians or other cardholders to cross-hospital

boundaries. Because physicians must have rights to practice at particular hospitals, granting agencies would be required to validate physician certification prior to issuance of a temporary id.

Figure 2 Web interface and database fields (see online version for colours)

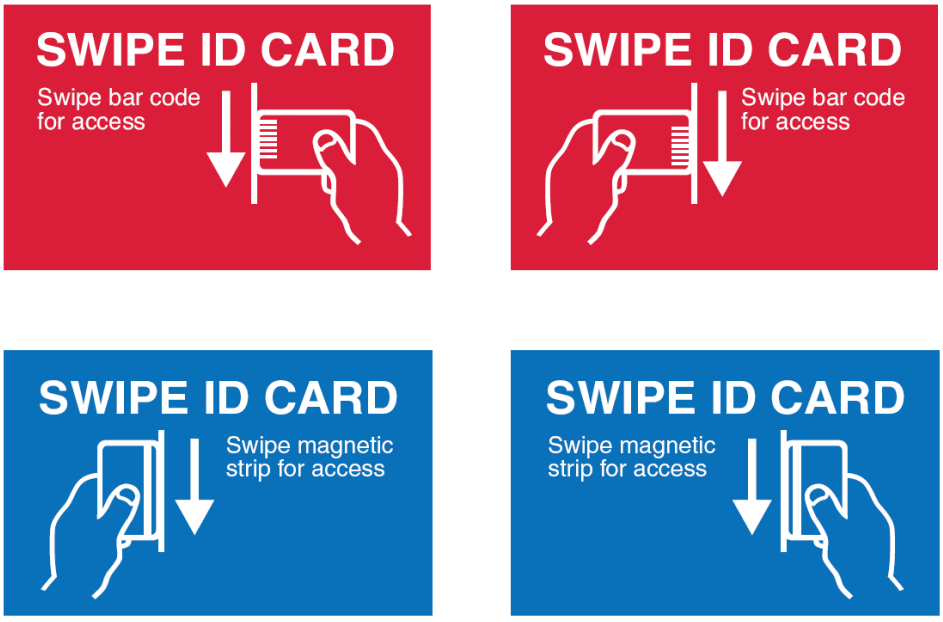


Fire/EMS agency administration of the system is similar with the exception of the affiliation process. All agency personnel that require access to the ED during normal operation are automatically affiliated with every hospital on the system, since they previously had access to the EDs as a group through then-current access control methods. Individual hospitals have the ability to grant access to Fire and EMS members into additional areas of the hospital on a case-by-case basis.

Badging workstations have a computer and monitor, an automated camera system, a barcode/magnetic stripe reader, and a badge printer. Stations have been deployed to several hospitals and other agencies throughout the city and surrounding areas to simplify the logistics of issuing badges. Emergency Management agencies or hospitals receiving out-of-area personnel, volunteers or visitors, may issue badges to those personnel on arrival and programme their access as appropriate.

Use of the system by a badge-holder is straightforward. Color-coded signs were placed at locations where the badge may be used; indicating which type of access control system controls the entrance. Magnetic stripe readers display a blue sign depicting a badge-holder swiping the card long edge down in the reader. A matching blue stripe running along the long edge of the card next to the magnetic stripe provided additional assistance. Barcode readers display a red sign depicting a badge-holder swiping the badge short edge down in the reader. A matching red stripe running along the short edge of the card on top of the barcode allows for easy identification. Labeling of the card readers is shown in Figure 3.

Figure 3 Labels on card readers (see online version for colours)



8 Infrastructure management

The information technology at the core of the system is maintained with standard best practices. The database and web-based application undergo daily backup with off-site rotation of storage media so that historical information is preserved. For security, all activity on the system is logged. Penetration attempts and suspicious activities are flagged for administrator investigation. Firewalls and intrusion detection systems serve as the front line of defense, with regular security evaluations allowing for the elimination of possible threats before they are exploited.

9 Future applications

At the time of this writing, the entire system was in place in the San Antonio area: all region hospitals had access control systems, the application and database was operational, and badges had been issued to 2600 physicians and approximately 2000 EMS personnel. The system had just 'gone live' with minimal irregularities. As funds become available, hospitals will be able to extend the uniform badge to their own employees in nursing and support functions.

The Alamo Area Council of Governments has also adopted the uniform ID badge for first response agencies throughout its 12 county area (this area partially overlaps TSA-P).

The City of San Antonio is further developing the badge to be part of a two-factor biometric authentication capability and incorporating its use in the SAFD Incident Command System. The University of Texas at San Antonio has received a $100K grant to demonstrate the use of biometric authentication and incorporation of the badge system with SAFD information systems. This system will be compatible with FIPS 201 standards in the event the City of San Antonio adopts smart card badging.

Deployment of the badge to Fire/EMS agencies in the rest of the 22-counties of TSA-P will proceed as funds become available.

Finally, the San Antonio Uniform ID Badge programme is being integrated with a parallel effort by the DHS. DHS has created a First Responder Authentication Credential (FRAC), currently being implemented for First Responders, Response Support, and Critical Government personnel in the National Capital Area. The FRAC has substantial physical and system similarities to the STRAC/BCMS uniform ID; however, the FRAC is a smart card embedded with an Integrated Circuit Chip (ICC) capable of Public Key Enabling (PKE) data. It reflects the Federal Information Processing Standard 201 (FIPS 201) (NIST, 2006), issued by the National Institute of Standards and Technology (NIST) as directed by Homeland Security Presidential Directive 12 (Bush, 2004). This standard specifies the architecture and technical requirements for a common identification standard for the Personal Identity Verification (PIV) of Federal Employees and Contractors. FIPS 201 defines a process to issue secure and reliable forms of identification based on sound criteria for personal identity proofing, registration, and issuance. FIPS 201 specifies use of identity credentials with ICCs that resist identity fraud, tampering, counterfeiting, and terrorist exploitation. These identity credentials can be rapidly authenticated electronically and are to be issued only by providers whose reliability has been established by an official accreditation process.

The identity proofing requirements remain the responsibility of the local jurisdictions but must meet a basic level of identity assurance in accordance with the Federal Bridge Certificate Authority (FBCA) Levels of Assurance. Additionally, the FRAC supports the integration of baseline critical skill sets (attributes) as defined in the National Response Plan's (NRP) National Incident Management System's (NIMS) 15 Emergency Support Functions (ESFs) (DHS, 2004), or the National Infrastructure Protection Plan's (NIPP) 17 Sectors (DHS, 2006). Most of the San Antonio badge database contains information that would be classified as 'attributes' on the FRAC.

Development of the phase two STRAC/BCMS uniform ID badge will follow the FIPS 201 identity credential issuance, architecture, topology, and technical requirements. Implementation of a FIPS 201 technically compliant credential, the FRAC, for First Responders, Response Support, or Critical Government personnel will enable interoperability not only with local jurisdictions, but also the Texas National Guard, USA Coast Guard, and all federal emergency response officials in compliance with HSPD 12. The STRAC/BCMS team will coordinate with DHS/NCRC to ensure future interoperability/compatibility through participation in a near future pandemic exercise/demonstration.

10 Discussion

This uniform badging project was developed in a 22-county region that has one of the most complex, inclusive, voluntary, trans-jurisdictional and trans-organisational medical disaster planning systems in the nation. This level of cooperation, at the highest levels of the organisations involved, is fragile and requires constant attention and transparency. Successful projects such as the uniform ID are also a powerful tool for building regional collaborations. A key factor in our success was the emphasis on consensus-driven decisions, which ensured buy-in from all participants. Another is the technology neutral system, which supports future changes in technology by using the agency driven back-end. Because the system uses a single centralised database for authentication, multiple copies of id badges could not but used. In addition, each badge contains a unique encrypted code that is used to 'kill' unauthorised or duplicated ID cards.

To create a uniform ID badge system in another area, we believe the following steps would be appropriate.

Step 1 Define the user community. What professional groups will use the system initially? Will the system be purely medical or will the responder community use it as well? Will it reside in one jurisdiction or across a region?

Step 2 Define requirements. The requirements we designed are a good starting point for discussion; other user communities may add or subtract according to local needs.

Step 3 Study existing access control infrastructure and identify gaps. Do all users have entry control systems? Do these cover all doors and gates that need to be covered at each facility? What types of systems are used? What access mechanisms (bar codes, magnetic strips, RFID chips, *etc*.) need to be included on a uniform badge for present and future compatibility across the area?

Step 4 Identify who will 'own' the system—who will be responsible for funding, administration and maintenance? Also, identify a project manager for organising and installing the system. The 'owner' and project manager may be different people. In our area, the STRAC/EHDG Hospital Security Committee is the 'owner' but the BCMS did much of the start-up project management, in close collaboration with the STRAC: a local vendor developed the database using national credential standards produced by Federal Emergency Management Association – National Emergency Responder Credential System.

Step 5 Confirm agreement of all users to commit the necessary resources to conform to the system's physical and administrative requirements and to use the system. This must be done at senior administrative levels since the project will most likely involve multiple departments in the hospitals, *i.e*. security, physician services, human resources, facility/plant maintenance, *etc*.

Step 6 Establish start-up funding. The STRAC/EHDG provided funding from HRSA bioterrorism hospital preparedness grants, which will be less available in the future.

Step 7 Define database fields.

Step 8 Acquire and install access control systems where needed.

Step 9 Acquire server, database software and badge printers.

Step 10 Test and refine any deficiencies noted in the system.

Step 11 Train agency-level badge administrators.

Step 12 Deploy system.

Much work remains in determining appropriate data fields for individual qualifications. There has been much enthusiasm for using such a platform for carrying information on which to base emergency credentials for out-of-area volunteer responders, whether physicians or others. Caution is in order. The term 'credentialing' has a different meaning for physicians than for other professional groups. First responders use the word simply to indicate that they are who and what their badge says they are, such as a Basic EMT or a Paramedic, according to a national standard for what those words mean. Physician credentials are granted by individual hospitals through a detailed process dictated by both JCAHO and local policies, based on the physician's specialty training, currency and performance history. The credentials are specific down to individual procedures, such as specific surgical operations, and care of specific conditions. They are highly sensitive information, especially if a physician's credentials were limited or revoked for alleged poor performance. Furthermore, information as detailed as a physician's credentials may not be necessary or appropriate for inclusion in the uniform ID badge database. What information should be included is currently being discussed.

Even for non-physicians, the validity of training information and other certifications is currently on the honor system. There is no mechanism for verification at the system level that an individual has completed specific training or that their training is current. However, in its present state of development, the uniform ID badge has already demonstrated that it meets a large and complex set of requirements from a large

and complex set of users in a uniformly satisfying way. Such systems will improve safety, security and accountability for hospitals and emergency responders wherever they are adopted.

References

Ahn, G.J. and Lam, J. (2005) 'Managing privacy preferences for federated identity management', *Proceedings of the 2005 Workshop on Digital Identity Management*, pp.28–36.

Autrey, P. and Moss, J. (2006) 'High-reliability teams and situation awareness: implementing a hospital emergency incident command system', *JONA: The Journal of Nursing Administration*, Vol. 36, pp.67–72.

Bush, G.W. (2004) *Homeland Security Presidential Directive/HSPD-12 Subject: Policy for a Common Identification Standard for Federal Employees and Contractors*, in T.W. House (Ed.).

Cieslak, T.J. (2003) 'Lessons learned', *Disaster Management & Response*, Vol. 1, pp.98–99.

DHS (2004) *National Incident Management System*, US Department of Homeland Security.

DHS (2006) *National Infrastructure Protection Plan*, US Department of Homeland Security.

Hanfling, D., Schafer, B. and Armstrong, C.W. (2004) 'Making healthcare preparedness a part of the homeland security equation', *Topics in Emergency Medicine*, Vol. 26, pp.128–142.

NIST (2006) 'Personal Identity Verification (PIV) of Federal Employees and Contractors – Federal Information Processing Standard 201', http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf, National Institute of Standards and Technology, Department of Commerce.