Tivoli

Business

Tampa General Hospital with 988 beds and over 6, 000 employees, wanted to Improve Its user Identity and access management processes to comply with Health Insurance portability and Accountability act requirements and improve operational efficiency. The hospital's disparate systems and processes for provisioning employees with access privileges had increased risk.

* Tampa General sought to better manage and track employee access to administrative and clinical applications; significantly reduce the number of passwords an end user needs to remember; and automate how employees are provided with access to Its mall clinical system.

The hospital engaged Prolific, anIBMPremier Business Partner to design a customized solution using IBM[email protected]to implement a new management process. * The new solution integrates with the hospital's human resources records and automatically provides security access to most employees. * The hospital engaged Prolific, an IBM Premier Business Partner to design a automatically provides security access to most employees.

The solution centralizes the hospital's management of user identities and access rights across heterogeneous * IT resources and gives Tampa General something it never had before: precise knowledge and control of who has access to applications.

“ This solution Is used to manage security access throughout the entire employee life cycle, Prolific security practice leader. “ It can automatically create and modify access based upon a person's organizational role and eliminate user access for terminated personnel.

The solution has auditing and control features to enforce compliance to hospital policy, minimizing the risk of personnel having unauthorized access to applications. ” Tampa General now has tight control of access to Its mall clinical system and tenant data, which lets it comply with security and privacy regulations and enhance patient care. The Prolific and IBM solution currently manages access for over 6, 300 users? including the hospital’s clinical professionals and billing and registration staff ? to Tampa * General’s main clinical system, which handles most of the hospital’s functions.

“ The solution makes sure people have need-only access to applications, which Is a HAIFA requirement,” Joseph said. This Includes ensuring that access Is disabled when an employee is terminated from a job? which often was not the case when access management was done manually. The solution also detects if an outsider hacks into the system and creates account for himself, or if a hospital employee creates accounts and gains unauthorized access to applications? enabling a quick response by hospital authorities.

Plus, It has eliminated shared user accounts and login IDs, so the hospital can now effectively track who Is accessing systems and * What HAIFA? * The Health Insurance Portability and Accountability Act of 1996 (HAIFA) enacts sweeping changes in how the healthcare professions handle the administrative details of their practices, and contains a broad and stringent framework for the rivalry and confidentiality of personally identifiable health information. This Federal statute was enacted as Public Law 104-191. Further information regarding this act can be found at the Department of Health and Human Services (HASH) website.

What issues are addressed by HAIFA? * The Administrative Simplification provisions of HAIFA (Title II of the Act) require HASH to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. Covered entities must comply with the technical standards and data sets adopted by HASH. HAIFA also addresses the security and privacy of health data, and establishes stringent procedures that covered persons and entities must follow in obtaining and disclosing personally identifiable health information. Transactions are activities involving the transfer of health care information for specific purposes. Under HAIFA Administration Simplification if a health care provider engages in one of the identified transactions, they must comply with the standard for that transaction. HAIFA requires every provider who does business electronically to use the same health care transactions, code sets, and identifiers.

HAIFA has identified ten standard transactions for Electronic Data Interchange (DE’) for the transmission of health care data.

Claims and encounter information, payment and remittance advice, and claims status and inquiry are several of the standard transactions. Review all of the electronic transactions required by HAIFA (listed in the box to the left of this page) and determine what transactions are used by your office. * Code sets are the codes used to identify specific diagnosis and clinical procedures on claims and encounter forms. The COP-4 and ICED-9 codes that you are familiar with are examples f code sets for procedure and diagnosis coding.

Other code sets adopted under the Administrative Simplification provisions of HAIFA include codes sets used for claims involving medical supplies, dental services, and drugs.

* other HAIFA * Administrative Simplification Requirements * Privacy Requirements: The privacy requirements govern disclosure of patient protected health information (PHI), while protecting patient rights. * Security Requirements: The security regulation adopts administrative, technical, and physical safeguards required to prevent unauthorized access to protected health care information.

The Department of Health & Human Services published final instructions on security requirements in the Federal Register on February 20, 2003. The deadlines for compliance are April 20, 2005, and April 20, 2006 for small health plans. * National Identifier Requirements: HAIFA will require that health care providers, health plans, and employers have standard national numbers that identify them on standard transactions.

The Employer Identification Number (NINE), issued by was adopted effective July 30, 2002. The remaining identifiers, such as the national patient identifier, are expected to be determined in the coming year.