TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

AFFORDABLE SOLUTIONS FOR IDENTITY & ACCESS MANAGEMENT FOR **HEALTHCARE**

WITH THE EMERGENCE OF VARIOUS STANDARDS, ESPECIALLY HIPAA, INFORMATION SECURITY HAS BECOME A TOPIC OF INTEREST IN THE HEALTHCARE SECTOR. ACHIEVING ADEQUATE INFORMATION SECURITY REQUIRES EFFECTIVE AND ACCURATE MONITORING OF EVERYONE WHO HAS ACCESS TO CONFIDENTIAL INFORMATION SUCH AS PATIENT DATA.

SECURE AND COMPLIANT USER MANAGEMENT

Many healthcare providers are conscientiously involved in dealing with privacy issues and managing sensitive information. Processes such as the recording of all changes for audit purposes, the use of complex passwords, the disabling of group accounts and the implementation of effective out-of-service procedures are becoming commonplace in healthcare organizations. The trend towards individual nurse logon accounts rather than shared accounts is becoming commonplace as well. These additional requirements increase the already heavy burden on the IT department. Implementing an automated Identity & Access Management system will help your organization to arrange processes in a more efficient way, reduce the workload, and improve SLAs and to cut costs.

Tools4ever's software solutions are deployed by a large number of hospitals, mental healthcare facilities and elderly care organizations throughout North America for the following:

- User Account Management
- Password Management
- Self Service Password Reset (SSRPM)
- Single Sign-On (SSO)

USER ACCOUNT MANAGEMENT

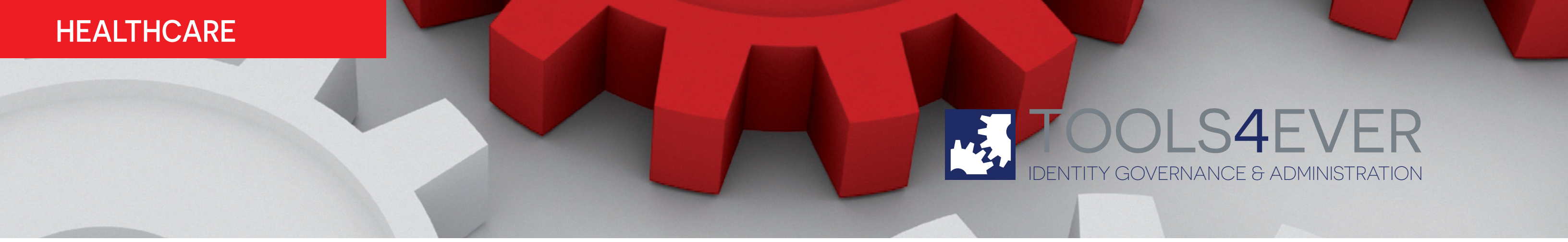
Tools4ever's UMRA solution offers healthcare organizations the possibility to streamline their user account management process e.g. the management of access privileges to systems and applications during an employee's tenure. This is normally achieved through:

Auto Provisioning:
UMRA Auto Provisioning is capable of automatically creating a user account via connectors with your HR system such as Lawson, Meditech, McKesson, Kronos. There are also connectors available to handle the creation of accounts in various other systems, such as medical systems, pharmacy systems and radiology systems. When an employee leaves service, the connector with the HR system will automatically initiate a disable procedure for the user account, so that the person in question will no longer have access to your network. Please refer to the back of this flyer for a list of available connectors.

Role Based Acces Control (RBAC):
Using RBAC, healthcare organizations can prevent employees from gaining unauthorized access to sensitive information. UMRA supports RBAC, so that organizational roles can be efficiently translated into user-specific access privileges.

Self-Service & Workflow Management:
If employees require access to network resources such as shares, applications, distribution lists, functional mailboxes, etc., they can request access themselves using a Self-Service system. The system will automatically create a workflow for the required approval and implementation of access privileges.

> ‘UMRA HAS SAVED US TIME AND MONEY. WE HAVE CUT OUR ADMIN TIME FOR NEW USERS BY 80%, AND THE WORK IS DONE BY NON-ADMINS.’
>
> JON POSTIGLIONE, SYSTEM ADMINISTRATOR AT PROVIDENCE HOSPITAL



PASSWORD MANAGEMENT

Standards for best practices suggest the use of complex passwords. However, the introduction of complex passwords often results in implementation issues such as password reset calls, end-user complaints and lock-outs during office hours. The following solutions are available to prevent these issues:

Self Service Reset Password Management:
Self Service Reset Password Management (SSRPM) offers end-users the possibility to reset their passwords without placing a call to the helpdesk. By answering a number of questions, they can have their password reset, or their account unlocked, at any time without intervention.

Password Complexity Manager:
The complexity rules in Microsoft Windows are limited and far from user-friendly. Password Complexity Manager supports a wide variety of complexity rules and offers end-users instructions to allow them to comply with the required password complexity.

Password Synchronization Manager:
Password Synchronisation Manager (PSM) allows users to synchronize passwords across various applications to minimize the number of passwords that users have to remember.

SINGLE SIGN-ON

Healthcare providers are eliminating shared user accounts for compliancy reasons. This makes the login procedures for end users more complex and time-consuming; they are required to remember multiple login procedures and use highly complex passwords for security reasons.

Single Sign-On (SSO) caters to this development by requiring users to log in only once. They will no longer have to enter passwords for each authorized application.

Fast User Switching:
Login procedures can be further simplified by combining Fast User Switching with a user badge. In this way, users can obtain access to applications by inserting their smartcard. They can log out by removing their pass, so that the computer becomes available for the next user.

Follow-Me:
An addition to Fast User Switching is the Follow-Me principle, which allows users who have opened applications on Citrix and/or Terminal Server to continue their work on another computer. This results in considerable time savings, particularly in the case of specialists who make their rounds along departments and need to have access to their data via various computers.

OUT-OF-THE-BOX CONNECTORS

Tools4ever's UMRA solution offers out-of-the-box connectors for various applications and systems inside your healthcare organization containing user data. Examples are Active Directory, Exchange, hospital information systems, access systems and various other internal or hosted systems. The following connectors are among those currently available:

- Meditech
- Lawson
- GE Centricity
- Kronos
- McKesson
- Kronos
- SAP HCM
- SAS
- PeopleSoft
- InfoSys
- Boston Workstation
- Remedy
- Oracle Financials

For a complete overview of our 130 connections, please visit our website www.tools4ever.com