
A Case Study on Stamford Hospital

Improving Caregiver Productivity and Protecting Patient Information Through Ease of Access

June 2006



Winner!
Two Years in a Row
Best Identity Management
Best Single Sign-On
Best Two-Factor Authentication



info@encentuate.com

www.encentuate.com

Table of Contents

Executive Summary.....	3
Stamford Hospital – Organizational Overview.....	5
Project Description – Problem Definition.....	5
Project Description – Business Objectives.....	6
Project Description – Solution	7
Project Description – Technology.....	8
Cost and Benefits	9
Transportability	11
Appendix – Sample Clinical Workflow	12
About Encentuate	15

Copyright Notice

© 2004-2007 Encentuate®. All rights reserved.

The contents of this whitepaper are furnished for informational use only, are subject to change without notice, and should not be construed as a commitment of any type by Encentuate. Encentuate assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. Encentuate will not be liable for direct, indirect, special, incidental or consequential damages, as a result of reproduction, modification, distribution or other uses of this whitepaper.

Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) has set strict security standards for protecting confidential patient information. Unfortunately, achieving balance between mandates of proper security practices and the need to provide fast access to patient information has consistently presented many challenges for healthcare providers throughout the country.

The case study describes the challenges faced by Stamford Hospital, a not-for-profit healthcare provider serving Stamford, CT with more than 300 inpatient beds and 2,300 employees, and how Encentuate's healthcare identity and access management (IAM) solution helped Stamford achieve the proper balance between ease of access for caregivers and adequate security compliance.

Benefits of Encentuate's healthcare IAM solution at Stamford Hospital include:

- Improved quality of patient care via greater than 85% reduction in time-to-patient information
- Higher caregiver productivity via single sign-on/sign-off using existing building access badges
- Patient information protection via two-factor authentication and flexible desktop security policies
- HIPAA compliance via user-centric audit tracking and unique user logins
- Improved efficiency of IT administrators via centralized management of users, security, and workflow policies

The study also highlights the universal nature of the access and security problem and recommends best practices and a comprehensive IAM solution for healthcare providers.

Improving Caregiver Productivity and Protecting Patient Information through Ease of Access

Stamford Hospital – Organizational Overview

Stamford Hospital is a not-for profit healthcare provider serving Stamford, Connecticut and the surrounding communities for more than 100 years. The hospital is a community teaching facility with more than 2,300 employees and 300 inpatient beds in medicine, surgery, obstetrics/gynecology, psychiatry, and medical/surgical critical care units. Its mission is to provide, together with its physicians, a broad range of high quality health and wellness services focused on the needs of its communities. Stamford Hospital has affiliations with the New York-Presbyterian Healthcare System and is a major teaching affiliate of the Columbia University College of Physicians and Surgeons.

Project Description – Problem Definition

The Health Insurance Portability and Accountability Act (HIPAA) has increased the level of awareness and set the standard for protecting confidential patient information. Unfortunately, achieving the proper balance between ease of access and appropriate security has consistently presented many challenges for healthcare providers throughout the country. Further complicated by the aggressive migration toward an Electronic Medical Record (EMR), hospitals find themselves caught in the middle - between the mandates of proper security practices and the need to provide clinicians easy, unencumbered access to critical patient information.

Traditionally, hospitals across the country (like Stamford Hospital) have relied on the use of “generic accounts” within a shared workstation environment to ease the burden of access for caregivers. Against the wishes of the clinicians and medical staff, the hospital no longer was able to support this practice under the restrictions of HIPAA. Alternatively, Stamford Hospital was required to mandate the use of unique user IDs and passwords for all clinical users. However, as the hospital continues the aggressive march toward a digital medical record, the number of clinical applications continues to climb. Thus, increasing the number of user IDs and passwords caregivers are required to manage, remember, and enter to gain access to information required for the provision of effective patient care. This is a process that is often repeated as caregivers “roam” from patient to patient, seriously complicating workflow, productivity and ultimately taking time away from the patient.

To further complicate matters in this more restrictive environment, if a caregiver failed to “logout” of their application session, all subsequent users would be restricted from gaining access to that workstation. Again, HIPAA mandates that if a workstation is left unattended while a user is “logged in,” the workstation must lock after an appropriate amount of time has lapsed. Given that Stamford Hospital was unsuccessful in forcing its clinical users to adopt the discipline of “logging out,” many workstations would be left in a “locked state” obstructing access to an already limited resource. When this issue presented itself, the caregivers were forced to either find an alternate workstation or turn-off or reboot the workstation as to release the lock - a model that was completely unsustainable, and the source of much inefficiency and frustration throughout the organization.

This proliferation of multiple user IDs and passwords coupled with complex security policies created immense frustration for the caregivers. Common accounts and passwords would be posted in the unit so that all could gain access to patient information from a single user account (reminiscent of the generic accounts); users would falsely place “out-of-order” signs on workstations deterring others from interrupting their login session; battles would ensue from users staking claim to a shared workstation as their own. The very measure designed to protect access not only caused disruption and complicated workflow, but also served to actually weaken Stamford Hospital’s security posture.

Project Description – Business Objectives

Working with its medical staff leadership, the Stamford Hospital sought a solution that would enable it to more effectively balance the need for improved security while supporting the caregiver’s demand for quick and easy access to critical patient information. Traditionally security measures have consistently obstructed access and the contradiction presented a major challenge. Ignoring the challenge and reverting back to “generic logins” was not an option. Stamford Hospital’s staff wanted to discover an innovative solution, which enabled the hospital to “provide security through convenience” for our more than 1250 clinical and medical staff members. Accordingly, the team established the following objectives:

- Comply with HIPAA Security requirements
- Protect confidential patient information on shared workstations
 - Centrally secure and track access to electronic protected health information (ePHI) by eliminating generic logins
- Allow the caregivers “nearly transparent” access to patient information
 - Enable single sign-on (SSO) functionality

- Streamline workflows on clinical and personal workstations
- Provide seamless access to patient information in a clinical shared workstation environment (1,250 caregivers sharing more than 300 workstations)
- Leverage existing RFID badge technology (HID iClass) for employee identification and building access
 - Minimize costs and variables by leveraging an existing ubiquitous infrastructure presently in place for every employee and physician
- Ensure high availability and ease of use
- Support an aggressive enterprise rollout with minimal interruption and training

Specifically, the primary requirement was to implement an Identity and Access Management (IAM) solution that would secure access to confidential patient information while also streamlining clinical workflows. “As a CMO, my key responsibility is to make my physicians’ lives easier,” said Dr. John Rodis, CMO and SVP of Medical Affairs. “Our primary objective behind the implementation of an identity and access management solution was to significantly streamline and secure access to patient information in order to improve patient care and patient safety.”

Project Description – Solution

After evaluating several software providers, Stamford Hospital implementation team initiated a three-week pilot study using the IAM solution from Encentuate. The client software, which provides single sign-on and single sign-off, clinical workflow automation, and authentication management, was installed on eight client workstations in the most complex environment: the Emergency Department (ED). An Identity Management Server (IMS) was also installed to help IT administrators define user templates, manage user identities, and create workflow policies that are enforced by the client software. The server also provides comprehensive backup of credentials, loss management, audits and compliance reporting. For the pilot project, the IAM solution successfully integrated information access and physical access security with the employee ID badges (RFID HID iClass Photo Identification Badge). This allowed pilot users to simply tap their employee ID badge on an RFID reader and enter a 4-digit personal identification number (PIN) to gain access to the workstation and their application portfolio, including the hospital’s new MEDITECH HCIS, Fuji PACS, and McKesson HPF Document Imaging systems.

Following the successful pilot, the implementation team quickly built single sign-on integration for all applications. In less than ten weeks, the team completed the integration of more than 27 independent applications and automated all required clinical workflows. In the subsequent four weeks, over 1,250 clinical professionals, including medical, ancillary medical and nursing staff

were registered and trained on the use of the system. An enterprise-wide deployment was successfully completed in ten weeks. The result was all the members of the clinical staff (physicians, nurses, technicians, aids, etc) were able to gain access to more than 300 clinical workstations and the entire portfolio of clinical applications by simply tapping their employee badge and entering a 4-digit PIN. “We were extremely impressed with how quickly we were able to deploy the IAM solution throughout our hospital,” said Keith Ryan, CIO and VP of Information Services. “Unlike many IT solutions, which may take months to integrate, we were able to integrate all of our clinical users into our new IAM solution in a matter of weeks.”

Project Description – Technology

The Encentuate Identity and Access Management (IAM) solution leveraged existing HID iCLASS employee badge technology to combine physical and logical (i.e., information) access. The IAM solution provides single sign-on / sign-off to all applications, including graceful suspension and resumption of sessions. In addition to single sign-on, the solution reduces the “time to patient information” by automating workflows on clinical and personal workstations. The solution enables efficient sharing of clinical workstations through fast user switching, and provides walk-off security automation to protect workstations that are left unattended. The solution also provides the hospital’s IT team with a variety of user-centric auditing and reporting features, including a digital audit trail of users’ access events to workstations and applications.

Figure 1.0 on the next page represents the user-centric, server managed architecture of Encentuate’s Identity and Access Management solution. The AccessAgent securely authenticates the caregiver and provides access to healthcare information systems while simplifying and enhancing caregivers’ ability to access patient information. The IMS Server provides web-based, centralized identity and workflow policy management while ensuring compliance by providing user-centric auditing.

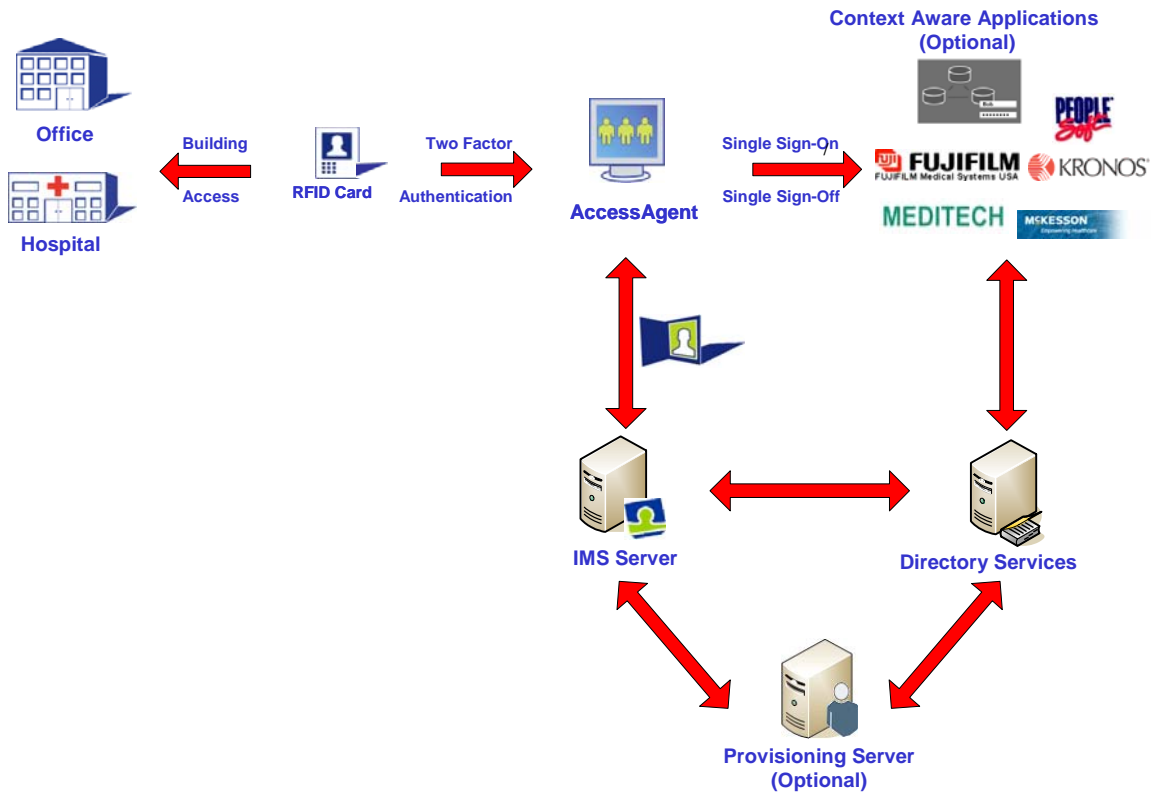


Figure 1.0 Encentuate Identity and Access Management Solution

In summary, the solution provided the following security benefits, while improving workflow and access to information in a completely transparent manner:

- Eliminate generic accounts
- Provide single sign-on / sign-off for caregivers and employees
- Automate clinical workflows
- Implement unique user identities and sessions
- Secure access to multi-user, clinical workstations
- Combine physical and information access through a single employee ID badge
- Audit access to all applications and provide consolidated reporting
- Provide centralized management of users and security policies

Cost and Benefits

The total capital costs to implement the Encentuate solution included the software licensing, hardware, and professional services. As mentioned earlier, the RFID badge technology was already in place supporting employee identification and building access.

As with all innovative solutions, the costs are very much overshadowed by the benefits. With the identity and access management solution, caregivers at Stamford Hospital can now experience fast access to patient information. Physician and clinical user satisfaction is at an all-time high. The IAM solution has dramatically improved caregiver workflow and productivity, allowing them to provide a better quality of care. "Time is of critical importance in a hospital, and as we are running from patient to patient, we don't always have the time to enter various passwords and remember to log-out from applications," said Valerie Neary, Director of Nursing at the Critical Care Services. "Encentuate aids in providing good patient care. More than anything, that is what matters in hospitals. It is invisible to the nurses and doctors and allows us to access patient information quickly, make informed decisions and protect the confidentiality of the patient."

"Clinical workflow on any nursing unit workstation was complex before Encentuate was implemented," said Dr. Michael Parry, Director of Infectious Diseases. "Now I sign on to my personal desktop using the ID badge, which makes the workflow very streamlined. I save a lot of time and dedicate that to making better clinical decisions instead of getting locked out of computers and remembering many passwords."

"With Encentuate, gaining access to patient information is now significantly easier as clinical users are only required to tap their badge and enter a 4-digit PIN," said Keith Ryan, CIO. "As a result, the 'time to patient information' has reduced by more than 85% per user session."

The solution enables IT administrators to now secure and track access to patient information; thus ensuring HIPAA compliance, without jeopardizing clinical workflow and ultimately patient care. "Our new IAM solution has eliminated our dependence on passwords and significantly reduced the password related help desk calls," said James Hodge, SSO Project Manager. "Due to the replacement of multiple passwords with one, the percentage of helpdesk calls related to password resets have reduced from a monthly average of 600 to 400 resulting in an annual saving of \$40,000. Additionally, doctors and nurses no longer share logins and passwords, and policy compliance has significantly increased to nearly 100%," adds the SSO Project Manager.

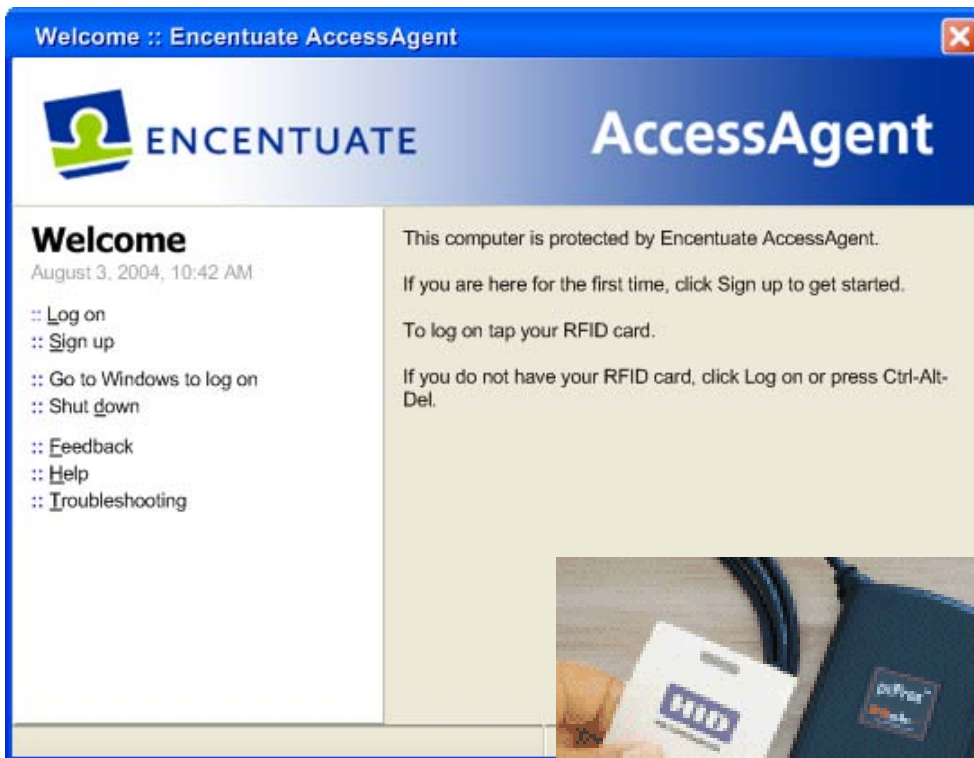
"Nurses no longer have to turn off workstations to log off other users and no one gets locked out!" said Mary Nielson, Clinical Educator. "Doctors and nurses have streamlined workflows and patient information is much more secure and easily accessible. "With Encentuate, we are able to enhance the quality of patient care and clinician productivity, while protecting the confidentiality of patient information." "With Encentuate, my physicians' life is easier and privacy of patient information is ensured," concluded Dr. John Rodis, CMO and SVP of Medical Affairs.

Transportability

As previously mentioned, HIPAA has set the standard for protecting patient confidentiality. Unfortunately, achieving these standards requires new and innovative ways to properly achieve the balance between ease of access and adequate security. This challenge is not unique to one organization, but is pervasive throughout every healthcare provider in the country. As the movement continues toward a fully digital environment, hospitals must find ways to secure the information while allowing for nearly transparent access in order to streamline the caregiver's workflow. "The solution delivers a complete roadmap for our future identity and access management requirements. This is a valuable solution that will result in higher productivity for both our medical and IT staff, allowing our caregivers to focus on delivering quality patient care," concluded Keith Ryan, CIO. "The solution is easily transportable to all healthcare providers, and should be considered at other hospitals and health systems throughout the country." This IAM solution is a comprehensive solution to a ubiquitous problem for healthcare. "As a leading healthcare provider, our goal is to deliver the best quality of patient care, improve patient safety, and protect patient information," said Brian G. Grissler, President and CEO. "Through Encentuate, we have been able to significantly improve our caregiver productivity and meet our goals of improving patient care and patient safety while ensure compliance with HIPAA mandates."

Appendix – Sample Clinical Workflow

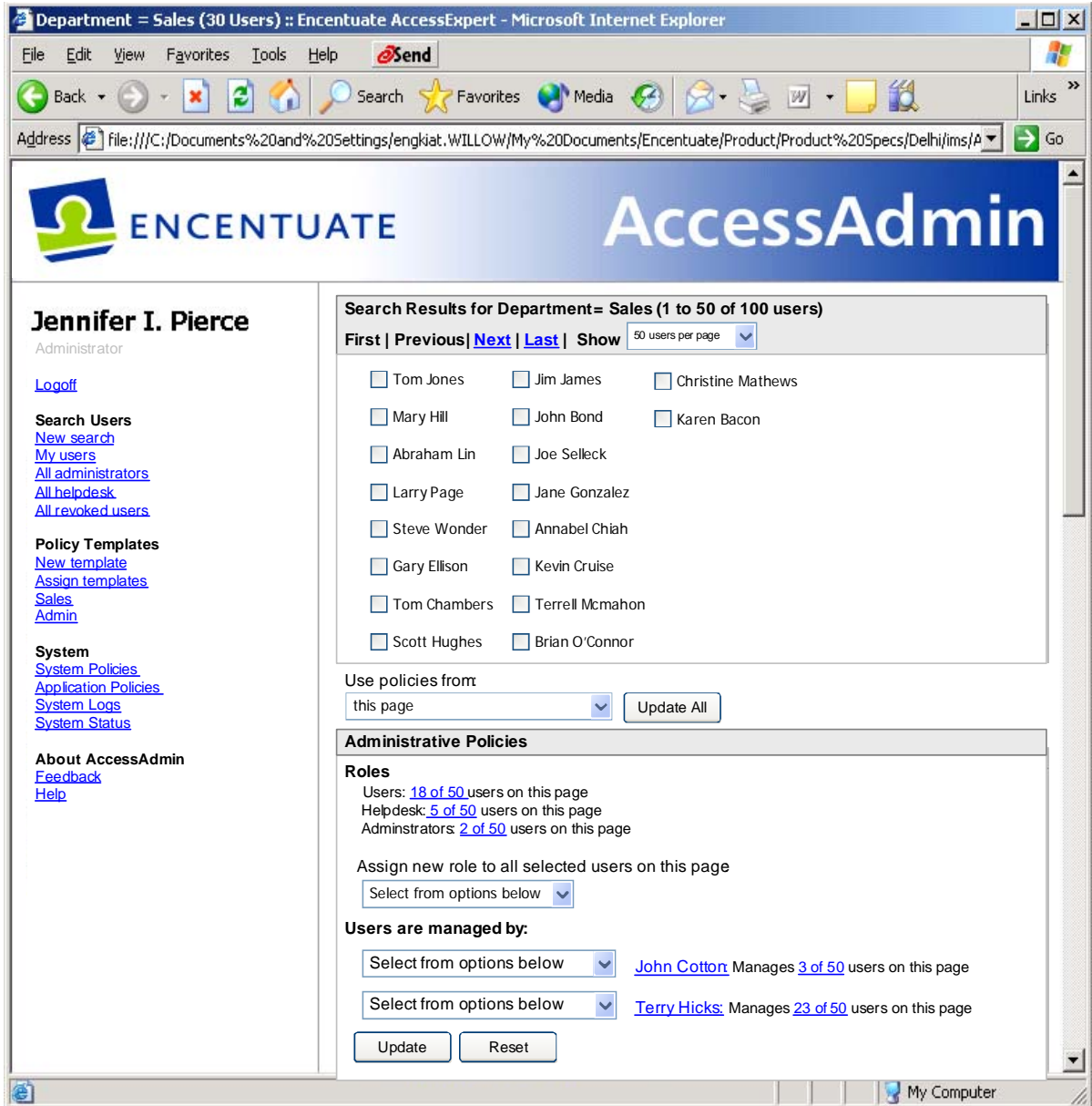
1. Caregivers walk up to a clinical shared workstation and tap their HID iClass building access badges and are presented with the following login screen. Time to patient information is reduced to 15 seconds compared to 120 seconds prior to implementing the solution.



2. Upon successful login, the caregivers can access any approved applications without entering additional user IDs and passwords. The IAM solution auto-fills all login screens with unique user credentials.
3. Caregivers tap their badge when they are done with the clinical shared workstation, or a time out will automatically be enforced on inactivity. This will automatically lock the screen or logoff the caregivers from their applications, ensuring HIPAA compliance while maintaining user convenience.



- 4. IT administrators use AccessAdmin, the web based administration console of the IMS Server to provide centralized identity and workflow policy management. The solution also ensures compliance by providing consolidated, user-centric tracking and reporting.



About Encentuate

Encentuate is a leading provider of enterprise end-point identity and access management solutions that help customers cost effectively simplify access to corporate information, strengthen security, and track compliance at enterprise end points without requiring changes to existing IT infrastructure. Encentuate is headquartered in Silicon Valley, Calif. and has offices across North America and in Singapore. Encentuate's customers span a range of industries, including healthcare, biotechnology, government and financial services. In 2007, SC Magazine named Encentuate TCI the **best identity management solution**. Previously, Encentuate was also recognized by SC Magazine as the **best single sign-on** and **best two-factor authentication solution**. More information about Encentuate is available at www.encentuate.com or by calling +1 866 362 3688.

Asia-Pacific

Tel: +65-6473-5110

Fax: +65-6473-5108

Europe

Tel: +44-20-7993-6351

Fax: +44-870-130-4568

North America

Tel: +1-650-413-6800

Fax: +1-650-649-1983