

# Achieving HIPAA Compliance at Clinivate with Two-Factor Authentication

Clinivate had to ensure its Clinitrak solution and outcome tracking capabilities met the strict security requirements of the Health Insurance Portability and Accountability Act (HIPAA).



## Clinivate

As a software solution developer for behavioral health providers, clinicians, and managers, Pasadena-based Clinivate had to ensure its Clinitrak solution, which makes it simple for authorized medical workers to benefit from secure real-time online billing, productivity, and outcome tracking capabilities, met the strict security requirements of the Health Insurance Portability and Accountability Act (HIPAA).

In order to be fully compliant with HIPAA, Clinivate had to incorporate two-factor authentication technology within Clinitrak. After researching available solutions and speaking with Matthew Tucker, Vice President of Sales at IT security solutions and services provider Pegasus Technologies, Clinivate selected CRYPTOCard's AuthEngine as the simplest and most cost-effective method of adding the two-factor authentication functionality required.

"We began researching all available solutions but the cost was extremely prohibitive," noted Terui. "Also, most did not provide the flexible functionality that would enable Clinivate to

provide its healthcare clients with high-level security without complicating the logon procedure for busy medical staff."

## Simple, Cost-Effective Two-Factor Authentication...Built Right In

Pegasus explained that CRYPTOCard had recently developed technology that was specifically designed to enable software developers to embed token-based, two-factor authentication within any custom application or environment, including websites, databases, and directories. In essence, AuthEngine would enable Clinivate to build two-factor authentication right into Clinitrak – giving Clinivate complete control over the authentication process, including system provisioning, enforcement, and workflow. This would make it simple for Clinitrak to address the authentication requirements of HIPAA.

"CRYPTOCard developed AuthEngine because it recognized that most people already have 95 per cent of the components they need for strong authentication in place," said Matthew Tucker, Vice President of Sales, Pegasus Technologies. "AuthEngine provides the remaining five per cent with far less

## Case in Point...

### The Clinivate Solution

- CRYPTOCard successfully secured Clinivate's real-time Clinitrak solution to HIPAA standards
- AuthEngine implementation delivered strong authentication to a unique application
- Eliminated the use of static passwords with Two-Factor Authentication

## Case Study

coding than building a bridge to a stand-alone authentication server,” Tucker continued.

Providing a major improvement in productivity and cost over traditional APIs that simply build a bridge between the custom application and a stand-alone authentication server, AuthEngine eliminates the need to purchase, install, and support a separate authentication server, and can be up and running in a couple of hours.

“AuthEngine proved easy to install, and it was clear from the outset that there was no comparable solution that could provide everything needed in one piece to make it simple for Clinivate to build two-factor authentication right into Clinitrak,” noted Terui. “With AuthEngine built in, if an agency has 50 users we simply initialize 50 tokens and send them to their administrators,” Terui continued. “As a result, it took no time at all for Clinivate to deploy the first 300 tokens to six agencies.”

AuthEngine’s flexibility also enables Clinivate to provide its clients with the ability to set multiple access levels so that an administrator can control the complexity of authentication to meet an agency’s specific requirements.

“When a new user needs access to the system, an administrator simply has to generate an activation code and then send the token along with a short instruction page to the user,” said Terui. “Then, once the user uses their token to generate a one-time logon password not only can the administrator be certain that the person attempting access to the system is who they say they are, but also that they can only gain access to appropriate areas of the system,” Terui continued. “It really is that simple.”

With the addition of two-factor authentication, Clinivate has been able to provide a solution that is not only HIPAA

compliant, but one that also meets the strict security legislations being implemented by L.A. County.

“L.A. County is mandating that all agencies that provide it with services have to utilize a system that incorporates EDI [Electronic Data Interchange] for submitting online claims,” said Terui. “As no other vendor’s technology presently includes two-factor authentication to positively identify the sender, Clinitrak is the only solution that can facilitate these electronic claims online,” Terui continued.

### Simple And Cost-Effective

By providing a simple and cost-effective method of adding two-factor authentication to Clinitrak, AuthEngine has enabled Clinivate to provide the user-friendly, secure real-time medical system access its clients’ demand, while simultaneously addressing critical HIPAA requirements.

“AuthEngine was a perfect fit for Clinivate,” concluded Terui. “As everything came in one easy-to-install package it provided the simplest and most cost-effective method to integrate user-friendly two-factor authentication within Clinitrak.”

### About CRYPTOCARD

CRYPTOCARD is a leader and innovator in the Network Authentication Industry. Its multi-awarded, much-lauded Two-Factor Authentication options include both a server based or ‘product’ solution (CRYPTO-Shield) and a Managed Authentication Service (CRYPTO-MAS). The combination allows organizations of any size and means to adopt a strong authentication policy. CRYPTOCARD is unique in the industry in their commitment to ensuring their products/ services work with any common network architecture including OS compatibility (Windows, Linux, Mac OS X), webserver flexibility (IIS, Apache) and database options (Active Directory, LDAP, Open Directory etc). Add to that the outstanding ‘out of the box’ interoperability with many top industry network solutions including Citrix, Checkpoint, Cisco and many more, and you begin to see how CRYPTOCARD has grown since its origin in 1989 to become a thriving enterprise doing business in more than 70 countries.



### CRYPTOCARD North America

340 March Road  
Suite 600  
Ottawa, Ontario  
K2K 2E4 Canada

Toll Free: 800-307-7042  
Tel: +1-613-599-2441  
Fax: +1-613-599-2442  
E-mail: [info@cryptocard.com](mailto:info@cryptocard.com)  
[www.cryptocard.com](http://www.cryptocard.com)

### CRYPTOCARD Europe

Eden Park, Ham Green  
Bristol BS20 0EB,  
United Kingdom

Tel: +44 870 7077 700  
Fax: +44 870 7077 711  
E-mail: [info@cryptocard.com](mailto:info@cryptocard.com)  
[www.cryptocard.com](http://www.cryptocard.com)

CRYPTOCARD and CRYPTO-Server are registered trademarks or trademarks of CRYPTOCARD Inc. in Canada, the U.S.A. and/or other countries. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.  
© 2006 CRYPTOCARD Inc.  
All rights reserved.

20070315