

# maverick™

## 2-Factor Authentication Scenario\* HEALTH CARE



\*Scenario is for illustrative purposes only.  
This is not a case study.



# maverick™

TOLL FREE / 888-266-1678 WEB / [www.MaverickSecure.com](http://www.MaverickSecure.com)

Hello and thank you for your interest in Maverick Secure.

In establishing Maverick I had a vision to build a company that everyone could be proud to work for, be associated with, and would want to conduct business. I believe we have achieved that goal and continue to aspire everyday to make that an on-going reality of continuous improvement. Here at Maverick Secure we are building a company that is run with integrity. Our ethos: SECURITY IS EVERYTHING. Our products, our service, and our mission will not be compromised. Our mission is to provide the most secure authentication process available on the market, and match that with the most affordable price point in the market.

The Maverick family is founded on several core principles:

- To stay ahead of hackers and rogue elements by providing the strongest, most secure, highly innovative and patented authentication processes available;
- To provide a great product at a reasonable price;
- To be responsible to our customers: your success is our success;
- To be responsible to our employees: we all work hard and so we should all share in our collective successes.
- To be responsible to this land that we all share: make every effort to create a sustainable product that will contribute to the health, vitality and industry of this planet;
- To invest in solutions that will enable the business community to grow and develop: businesses of all sizes are the backbone of our communities, our culture and our country.

Maverick Secure is fully invested in developing and protecting a work environment that rewards integrity and embraces diversity. We believe in quality service and support this with a strong work ethic. Here at Maverick Secure, we will not compromise integrity for profit. We will not discriminate on the basis of race, ethnicity, religious preference, sexual orientation or gender – rather, we will truly endeavor to embrace and elevate individuals who deliver on our core values. It's simple really: your success is our success. We believe in good honest work, and we will work hard to produce the tools, the solutions, and resources that make your task easier, more efficient, more profitable and most importantly, MORE SECURE.

On behalf of the Maverick family, I welcome you to learn more about our family of products, and to become our next Maverick Secure satisfied customer.

Thank you.

Patrick McNicholas  
Managing Partner



## Contents

Health Scenario	1
Welcome	2
Contents	3
Introduction	4
The Need	4
Case Scenario	6
Key Requirements	6
Challenges	6
Results	6
About Maverick Secure LLC	7

### Introduction

With the advent of computerization, people's health and medical records can now be collected, stored, analyzed and copied instantaneously. The petabytes of data can be utilized by various authorized organisations in order to serve the general public.

### The Need for a Strong 2-Factor Authentication

Nowadays, one of the main drivers for such solutions has to be a low TCO (total cost of ownership).

### Case Scenario

A hospital serving a large area is seeking to put up a portal that would make it easy for staff and patients to securely access the hospital's network and records databases.

### Key Requirements

Strongly protect confidential data by moving from traditional username-password authentication.

### Challenges

The new system has to be very secure but at the same time, simple, quick to deploy and easy to use.

### Results

The new system provides employees with a more secure access.

### About Maverick Secure LLC

- More secure, faster access to hospital records and cases.
- Secure and faster follow-up of claims and payments.
- Secure and faster ordering of critical clinical tests and processing of results.

## The confidentiality of medical records has become more paramount in today's increasingly online health care environment.

### At-A-Glance

#### Key Requirements

- Authenticate via a two-factor authentication system.
- Easy to learn and deploy.
- Flexible and multi-user authentication system.
- Cost effective.

#### Solution

- A strong token access system featuring exceptional two-factor authentication.

#### Results

- More secure, faster access to hospital records and cases.
- Secure and faster follow-up of claims and payments.
- Secure and faster ordering of critical clinical tests and processing of results.

### Introduction

With the advent of computerization, people's health and medical records can now be collected, stored, analyzed and copied instantaneously. The petabytes of data can be utilized by various authorized organisations in order to serve the general public.

Medicare relies on these data for claims and coverage. If you are applying for a job, your potential employers will use your medical data for determining whether to hire you and how much pay they will give you. They can even use your medical data to find out whether employing you will turn out costly in the long run. Hospitals use your medical data to find out the best treatment for your medical conditions, to file for reimbursement, to research for treatments and improved care, and reduce health care costs.

Consequently, medical records are an asset and the data centers housing medical and health data should be protected from unlawful intrusion.

Even if medical records are now mostly in electronic form, patients still have the right to complete privacy and confidentiality, a provision that makes it even more important to safeguard the security of sensitive information represented by patients' medical records. An attack on a hospital's medical data can prove disastrous for patients whose records are compromised, not to mention an enormous liability to the hospital, if the records fall into unscrupulous hands.

Hospitals should therefore have a system that controls and monitors access to their medical records and a way for determining if these are accessed for fraudulent purposes.

### The Need for Better Authentication When Accessing Hospital Records

Hospitals should, as a minimum, be able to control and log access to medical records and have the capability of tracing the access. Ideally, access to medical records should be more secure than a simple username & password combination which is using just the first of the three factors of authentication.

**By design, two-factor authentication schemes are:**

- Flexible and scalable – They can be used and tailored for small organizations or very large corporations with sites around the world.
- Easy to use and deploy – All you need is to insert the security token (smartcard, USB dongle, etc) into the appropriate reader and the system grants you access after you give the username, password, or additionally, the OTP. Since the concept is simple, deployment of security tokens all throughout the organization is faster and there are no steep learning curves. This means workflows are not impacted much, if at all.
- Cost effective – Ease of use and fast deployment and management (either centrally or distributed) and ubiquity allow greater savings in management, administration and system upkeep, thereby realizing greater returns on investment.

In a hospital setting, secure access to fast and easy systems could spell the difference between life and death—patients rely on quick, accurate diagnosis and treatment.

Using two or more authentication factors is better. The three factors of authentication are:

- Something you know – e.g., username, password and bits of personal information.
- Something you have – security token, smart card, USB dongle. Using both 'something you know' and 'something you have' two-factor authentication, for example, ATM transactions, is better because, even if someone gets your PIN or password, it's useless without the ATM card; conversely your ATM card is useless without the PIN.
- Something you are – voice, fingerprints, iris or retina scan, DNA or even brainwave patterns.

Using any two of these factors is called 'two-factor' authentication. The third factor, 'something you are' is still not a widely available option, so it is often only used in situations where people need the highest clearance, e.g. sensitive facilities and data like defence facilities or classified information that could make or break a company or a country.

For most people, two-factor authentication is a secure system depending on how it is implemented. ATM cards that require a 4 digit password are still vulnerable to brute-force attack because it just requires 10,000 tries to correctly guess the PIN although the risk is lessened because you can only have a few wrong tries before the ATM machine captures the card.

A better implementation of two-factor authentication is using a security token that generates a time-limited one-time password (OTP) good only for a minute or less. This way, even if attackers capture the correct username and password, say, by keylogging, they would still need to generate a correct OTP in the next access.

### Key Requirements

- System would use two-factor authentication for strong security against attacks;
- System should be able to authenticate both staff and outpatients (or their representatives) from a variety of operating systems and platforms.
- System would be easy to use and deploy without causing undue hassle with patients and staff.
- System needed to fit within the hospital's tight budget.

### Challenges

- Two-factor authentication was a good solution to the risks involved in accessing a hospital's electronic records system, both for staff and outpatients. Using a two-factor authentication system minimized the risk of unlawful access to one's medical records.
- The challenge was when to deploy the system to patients—when a new patient is signed in? Upon demand? What if the patient was in ICU? Hospital management formulated a deployment protocol while evaluating different authentication solutions that would best fit the hospital's requirements.

### Case Scenario

A hospital serving a large area was seeking to put up a portal that would make it easy for staff and patients to securely access the hospital's network and records database. Staff would use the portal to do research and identify possible patients qualified for possible testing and treatment, or for data exchange in furtherance of medical research. Outpatients, and their representatives, meanwhile could use the portal to email or chat with their attending physician, request or access their medical records where permitted by law, or follow-up claims and bills payments.

Access to this portal naturally required a strong two-factor authentication because a username and password authentication layer was just not reliable enough to be used where sensitive hospital records were concerned. The hospital reviewed several solutions offered by data security vendors.

### Results

The Maverick 2F™ solution was chosen. Deployment with hospital staff took just two man weeks. Deployment for patients was on an ongoing basis since some patients had been out of the hospital for years. Hospital management came up with a patient deployment protocol that accommodated all kinds of patients from outpatients, walk-in patients, to children and those who needed a caregiver.

An information page for learning how to use the system was made available at the hospital's website. This section needed no login. A comprehensive FAQ was also set-up, including information on laws pertinent to the disclosure of hospital records.

The first six months after the system was put in place saw a marked decrease in the time taken to process hospital bills and claims. There was also major improvements in the way resident physicians and medical scientists collaborated on the best diagnosis, treatments, and prognosis for patients, especially after the portal was linked to medical databases which provided state-of-the-art medical science knowledge.

Meanwhile, the system also proved beneficial for nurses since they didn't need to look up voluminous filing cabinets for patients' records. The hospital had deployed iPads and other tablet devices for convenient look-up and follow-up of a patient's medical and care regimen which negated the necessity to go back and forth to the nurses' stations as they made their rounds.

Since the hospital's different departments were also securely connected at the portal, it was also easier and faster for doctors to order more sophisticated imaging tests on behalf of their patients. Even X-ray results could be pulled up from the system without risk of a security breach.

### About Maverick Secure LLC

Maverick provides multi-factor authentication solutions to safeguard confidential digital records and data. It is applicable to industries including technology, Internet, healthcare, education, financial services, government, military and subscription services. Maverick's strong multi-factor authentication processes are your solution when passwords just aren't enough to protect your sensitive data from unauthorized users and hackers.

The Maverick brand is dedicated to providing the business community with a high quality and affordable alternative to the pre-existing/overpriced offerings currently available in the market. By providing user-friendly, scalable and seamless compatible technologies, our products match and very often exceed our competitors' products while remaining price sensitive, affordable and much greater offering value for money.

Maverick offers stronger security by leveraging the industry's leading multi-factor authentication processes in very unique and efficient out-of-band channel methods. By living up to its name, Maverick takes a unique "out of the box" strategic perspective in protecting our clients from the threats that surround us in this constantly evolving security-vulnerable world. Maverick provides an easy-to-use approach for users while providing the highest level of security as an overlay to existing business applications and systems.

The Maverick brand started out as Maverick Computers and was named as "One of the fastest growing computer companies in North America," "#1 Solution Provider" and the "#1 System Builder in North America based on growth (2004)," and "Server Innovation Award" by CRN Magazine for developing a virtually indestructible server. The company then launched a new sister company called Maverick Communications which was awarded "2005 North American System Builder Association – Business Innovation of the Year" for creating an integrated array of video, voice and data services that included what was then the world's fastest Internet access for consumers at 45mbps. Over the past five years a new division of the Maverick brand, Maverick Secure LLC., was launched to combat the ever-evolving and tenacious attacks of hackers such unauthorized access of data and the multitude of other security breaches have caused serious turmoil within the computer and associated industries. In 2009 Maverick partnered with IBM, the number one server company in the world for enterprise users, to develop the "Maverick SMART Server Powered by IBM." By utilizing the award winning hardware of Maverick Computers, the industry's leading authentication process of Maverick Secure and the online and business applications of IBM, Maverick is now positioned to deliver end-to-end solutions for businesses small and large. We believe we have brought together the perfect harmony of leading technologies to offer one of the most secure solutions that addresses issues related to password authentication.

## Contact Us

To learn more about how 2-Factor Authentication products, services, and solutions help solve your business and IT challenges please contact your local representative or authorized reseller.

### **Patrick McNicholas**

President

Maverick Secure, LLC.

[Patrick@MaverickSecure.com](mailto:Patrick@MaverickSecure.com)

[www.MaverickSecure.com](http://www.MaverickSecure.com)

772-216-9535 (Cell)

888-266-1678 (Toll-Free)

305-600-0772 (Miami)

917-470-9469 (New York)

415-424-4245 (San Francisco)

020-337-174-11 (London)

888-219-0113 (Fax)

GoToMaverick (SKYPE)

Maverick helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions.

Copyright © 2012 [MaverickSecure.com](http://MaverickSecure.com)  
All rights reserved.