HIMSS
Central & Southern Ohio Chapter
Ohio
transforming healthcare through IT™

Remote Access Authentication In Healthcare

Presented by Steve Dispensa
Chief Technology Officer, PhoneFactor

Agenda

- Intro
- Define Multi-Factor, importance, and role in compliance
- Multi-Factor obstacles and options in marketplace
- Market shift to phone-based methods
- PhoneFactor overview
- Case studies
- Questions

About PhoneFactor

- Founded in 2001
- SAS 70 Type II Certified
- Trusted platform
- Large scale/high risk verticals

Catholic Health Partners
Novant Health®
imprivata®
PROGRESSIVE®
OhioHealth
Children's Hospital Los Angeles
We Treat Kids Better
Microsoft® HealthVault™
Limitedbrands
Convergys
Outthinking Outdoing
Nationwide Children's Hospital™
Main Line Health
Well ahead.™
Citrix ready™
Lake Health
American Health Network
Scripps
Firelands Regional Medical Center
EMH Healthcare
Expert care. Exceptional caring.
Ready for IBM Tivoli software
Western & Southern Financial Group®

What Is Multi-Factor Authentication?

- A Second Layer Of Authentication Beyond User Name And Password
  - Something You Know - Password, PIN, Or Challenge Questions

    +
  - Something You Have - Phone, Credit Card, Or Token

    OR
  - Something You Are - Fingerprint, Retinal Scan, Or Other Biometric
- Stronger When Authentication Occurs Through Distinct Channels (Out-of-Band)

Why Is Multi-Factor Authentication So Critical?

- Authentication is the first line of defense against attacks
- Authentication “Touches” the user, so user experience is key
- The cost of a breach continues to grow
- Move toward electronic medical records, electronic prescriptions, automated healthcare systems, and mobile devices
- Not only is it best practice, industry regulation either recommends or requires it – HIPAA, State Pharmacy Boards, HITECH, ARRA, PCI DSS, etc.

The Role of Multi-Factor Authentication in Compliance

- Ohio State Board of Pharmacy
  - "Positive ID" cited in any rule regarding record keeping and drug documents
  - Sign in Ink = Sign Electronically = Positive ID = Multi-Factor Auth
- Title II of HIPAA Sets Specific Guidelines For Security
  - Protect "Electronic Protected Health Information" transmitted electronically over open networks (i.e. remote access)
  - Examples: Home health nurse, physician filling a prescription electronically, transmission of files from hospital to insurance provider, physician working remotely to hospital
  - Does not specifically require two-factor, but it is considered industry best practice

Multi-Factor Project Obstacles Can Be Daunting

- Employee Resistance
  - Physicians and staff do not want to carry an extra device
  - Work at multiple facilities with multiple devices
  - Tokens in particular can be difficult to read
- Large Scale Deployments
  - Often deployed to thousands of employees at multiple sites
  - Training and deployment are difficult to coordinate
- Unmanaged Equipment and Networks
  - Mobile devices, tablet PCs (iPad), computers and network connections are often not managed by the hospital's IT department
  - Supporting end user software or certificates can be a drain on IT resources

Multi-Factor Comparison

- Physical Tokens
  - Device that displays random 6 digit number in small screen for 30-45 seconds
  - Proven (15+ years) but vulnerable (RSA Breach + not OOB)
- SMS Tokens
  - Random digit sent to SMS enabled phone
  - More convenient than token but required to have SMS enabled cell phone/plan
- Certificates (PKI)
  - Deceptive financially: Less hard costs but higher on soft costs
  - Not true Multi-Factor “something you know and something your computer knows”
- Biometrics
  - Something you are
- Smart Card or Proximity Badge Readers
  - Typical option for “inside hospital walls” but not remote since physical reader required
- Phone Authentication
- Do Nothing – physicians’ favorite ☺

Market Shifts To Phone-Based Methods

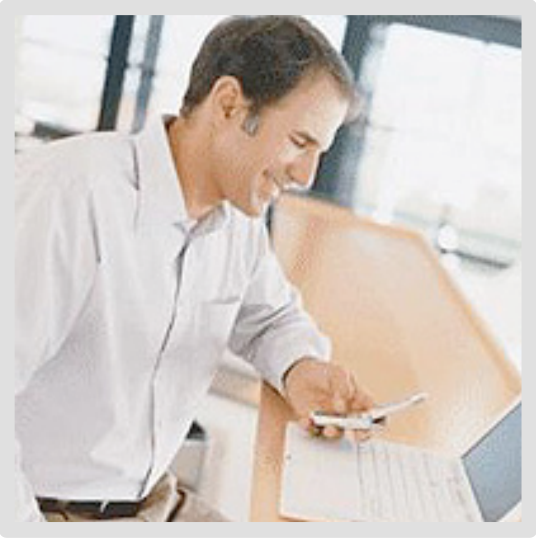
- Leading Analysts Firms Note The Shift To Phone-Based Authentication
  - “Phone-based authentication, like that provided by PhoneFactor, is predicted to comprise 61% of the multi-factor authentication market by 2014” – Goode Intelligence
  - “Handheld mobile devices will be the most-common physical form factor for new or refreshed user authentication implementations” - Gartner
  - “The support for phone-based authentication recently announced by Google (for Google Apps) and Facebook will only increase the rate of adoption.” – Gartner
- Phone-Based Authentication
  - Leverages the user’s existing phone as the trusted device
  - Telephones/phone numbers are extremely difficult to intercept or duplicate
  - Minimal impact on the user experience
  - Typically less expensive to implement and support than tokens

Benefits of Phone-Based Authentication

- User Adoption
  - User-friendly; everyone has a cell phone and knows how to use it
  - No end user training required, it is an extension of their everyday work/life flow
  - Accessible for users with disabilities
  - Works with any device from any location in the world – IT doesn't have to support multiple devices
  - User replaces his own phone from a local retailer rather than having IT ship him a new token, which would incur cost and downtime

Benefits of Phone-Based Authentication

- Out-of-Band Security
  - Uses a second channel for the second factor of authentication
  - Allows two-way communications to verify login or provide other input, such as a confirmation code
  - Allows playback and confirmation of transaction level details
  - Can also accommodate three-factor biometric voice authentication without special hardware (which biometrics typically require)
- Scalability
  - No devices to provision, mail, inventory, and replace
  - Easy to deploy for large numbers of geographically diverse users
  - Cost-effective to setup and maintain



Typical Healthcare Use Cases

- Physician and Employee Remote Access (Outside Hospital Walls)
  - Applications: Citrix, VPN, SSO, OWA
  - Key Benefit: High physician adoption rates + OOB increased security
- Board of Pharmacy Requirements
  - Applications: Citrix, SSO, EMR
  - Key Benefit: Approved and proven with OH Board of Pharmacy
- Third Party Vendors
  - Applications: VPN
  - Key Benefit: Eliminate device management for non- employee population
- Web Portals
  - Applications: Patient, physician, and employee web portal (i.e.: Microsoft HealthVault, PeopleSoft)
  - Key Benefit: Cost effective + scalable + no device management

imprivata™ | Microsoft Office Outlook Web Access | CISCO | CITRIX ready™ | Ready for IBM. Tivoli. software

PhoneFactor's Phone-Based Multi-Factor Authentication

- No tokens for users to carry and track
- No software or certificates for end users to install
- No hardware or devices to purchase and manage
- Works with any phone, anywhere in the world
- Supports multiple phone numbers with call rollover
- Can be setup in minutes for thousands of users
- No end user training is required
- Automated enrollment and user self-service

Two Easy Out-of-Band Authentication Methods

Step 1:

User logs into any application using their standard username and password.

Step 2:

Phone Call

Incoming
Call…
PhoneFactor
This is PhoneFactor. Please press the # sign to complete your authentication.

PhoneFactor places an automated phone call to the user. The user answers the phone and presses # (or enters a PIN) to authentication.

SMS Text

This is PhoneFactor. Please reply to this message with the following passcode to complete your authentication.

Your passcode is: 675532

PhoneFactor sends a OTP to the user in a text message. The user replies to the text message with the passcode (or the passcode and PIN) to authenticate.

Require a PIN to Authenticate

- **PIN Security**
  Add a third tier of protection by requiring users to enter a personal identification number (PIN) to authenticate. Even if an attacker had access to the user's phone, they could not authenticate without also knowing the user's secret PIN.

- **PIN Rules and Resets**
  Specify rules for PIN strength and expiration and allow users to change their PIN from the phone menu.

- Works with Phone Call and SMS Methods

- Defeats Call Forwarding Attacks

This is PhoneFactor.

Please enter your PIN followed by the # sign to complete your authentication.

Case Study: Ohio Health

Goal: Find a true two-factor solution to replace 4,300 RSA SecurID tokens that required less overhead and provided a more positive user experience.

- About OhioHealth:
  - OhioHealth is a large network of 17 hospitals and numerous other clinics and facilities serving Central Ohio. They have 2,500 physicians and 15,000 employees.
  - OhioHealth had been using RSA tokens to two-factor physicians and other staff for remote access into their electronic medical records. This had proven to be cumbersome and expensive.
- They transitioned away from security tokens to PhoneFactor. The results:
  - Increased efficiency and user satisfaction
  - Significant costs savings
  - An unchanged workflow
  - Regulatory compliance – HIPAA and Ohio State Pharmacy Board
  - Very little ongoing maintenance and user management

Our Host:
Catholic Health Partners

Goal: Replace Security Tokens in a key division to (1) Eliminate device management (2) Decrease costs (3) Improve physician experience.

- PhoneFactor client for one + years
- Previously using tokens
- Using PhoneFactor to secure remote access for physicians
- Their recommendation of PhoneFactor for you today:
  - ☑ Painless setup
  - ☑ Low maintenance
  - ☑ Positive accolades from physicians

THANK YOU

QUESTIONS

PhoneFactor

www.phonefactor.com

Re-evaluating your use of SecurID tokens after the RSA breach?

Check out our Token Replacement Program