



HIGH-ASSURANCE ID VERIFICATION BALANCES HEALTHCARE DATA SECURITY AND ACCESS

INTEGRATED AUTHENTICATION IMPROVES PRODUCTIVITY FOR
ALL STAKEHOLDERS WITH SYNCHRONOSS UNIVERSAL ID



SYNCHRONOSS UNIVERSAL ID FOR HEALTHCARE

SYNCHRONOSS UNIVERSAL ID: SECURE, CONVENIENT, COMPLIANT

In healthcare, every authorized stakeholder needs access to confidential data, from patients' protected health information (PHI) to hospital employee records. The challenge is to make that data conveniently accessible from within everyday workflows without sacrificing security.

In this digital era, too often that's a daunting task. And it's complicated by an increasingly mobile society, medical specialization, and continuing efforts to better coordinate care across providers using disparate information systems. The traditional, single-factor identification (username and password) still used by many of those systems doesn't resolve the complex identity and security challenges that healthcare providers face.

These factors and more have made healthcare a major target for fraud and identity theft. Studies show that 23% of all data breaches occur in the information-rich healthcare industry.¹ Such a breach can severely impact a patient's private life and an organization's reputation, while opening the organization to litigation liability and the imposition of significant regulatory fines.²

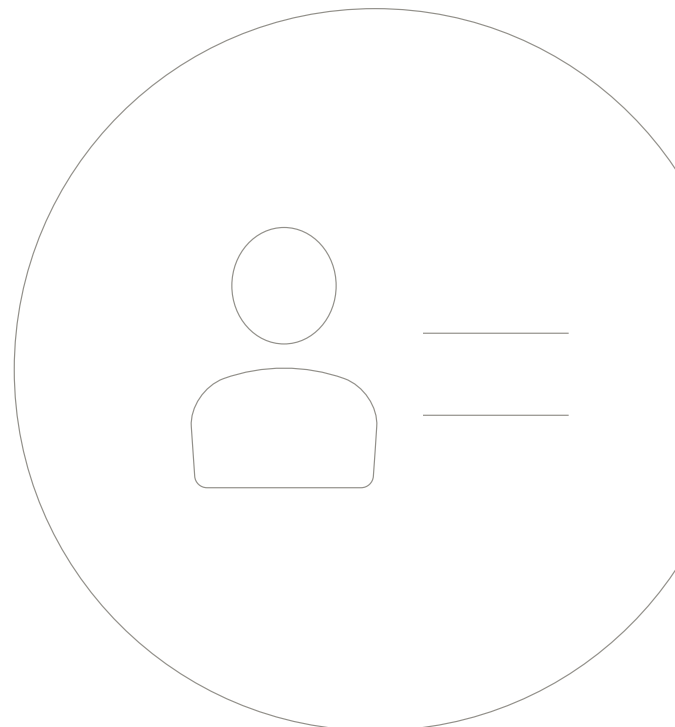
Synchronoss Universal ID is the solution. An integrated part of the Synchronoss Secure Mobility Platform, Universal ID enables secure multifactor authentication using cloud-based identity services designed and certified to meet the specific needs of the healthcare industry.

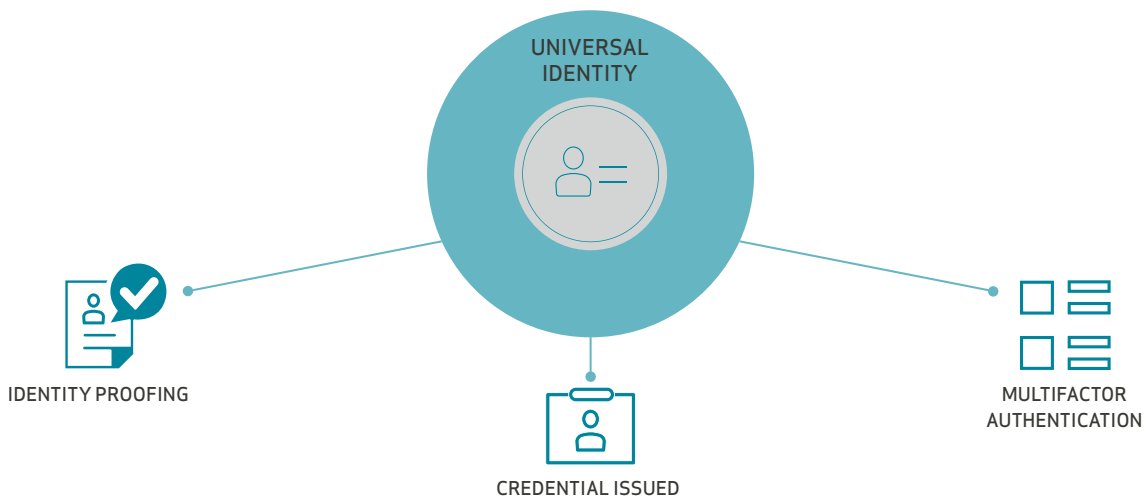
BENEFITS

- Easy verification of licenses and DEA numbers
- Fast, effective identity verification
- Increased security through convenient multifactor authentication—adding a randomly generated, one-time password on top of a traditional username and password
- Rapid deployment and scale on demand
- Reduced risk of medical identity fraud
- Reduced deployment and management costs
- Reduced support and help-desk costs

SYNCHRONOSS UNIVERSAL ID

ENABLES HEALTHCARE ORGANIZATIONS TO BALANCE DATA ACCESS WITH SECURITY, USING MULTIFACTOR AUTHENTICATION TO IDENTIFY AUTHORIZED USERS AND TO PROTECT AGAINST THE GROWING IDENTITY THEFT AND FRAUD THREATS





SECURE, COMPLIANT, COST-EFFECTIVE

REDUCE RISK

Universal ID provides a compliant identity-proofing process that authenticates the identity of an end user to the highest possible extent before credentials are issued. After the user's identity has been confirmed, a secure credential is issued, and the user can choose from several convenient multifactor authentication options. This greatly improves user satisfaction and reduces the risk of unauthorized access to patient data including PHI within an electronic health record (EHR), a pharmacy system, and others.

Importantly, Universal ID's integrated digital signature capabilities also leverage the identity verification process to ensure that only authorized providers are allowed to e-prescribe controlled substances, the availability of which has come under increasing scrutiny.

CERTIFIED, COMPLIANT ELECTRONIC PRESCRIPTIONS

It's critical to address compliance while providing a seamless workflow, enhanced productivity, and a positive user experience in the busy and complex healthcare environment. Unlike most commercial solutions available today, Synchronoss Universal ID is Federal Identity, Access, and Management (FICAM) certified to Level 3.

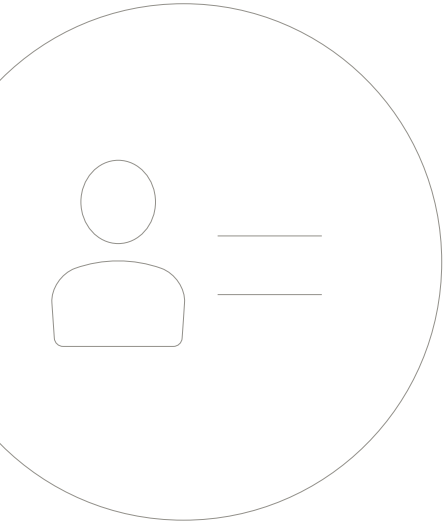
To achieve this certification, our verification processes and multifactor authentication have been designed to meet the rigid Level 3 authentication requirements created by the National Institute of Standards and Technology (NIST). This means that providers can securely, compliantly, conveniently, and confidently e-prescribe controlled substances as part of expanding e-health strategies.

CONTROL COSTS THROUGH A PREDICTABLE, CLOUD-BASED SUBSCRIPTION MODEL

Because Synchronoss Universal ID is completely cloud based, it eliminates capital expense for servers and software, and it provides a predictable pay-as-you-go model with a low monthly cost. Savings include:

- No on-premises dedicated infrastructure (servers, storage, and network resources)
- No hardware or software upgrade fees
- No additional administration or configuration costs
- No need to hire additional IT security staff
- Rapid deployment and expansion to accommodate new business growth
- Reduce help-desk costs with an end-user self-service portal

HEALTHCARE IS AN EXTREMELY ATTRACTIVE TARGET FOR HACKERS BECAUSE OF THE BREADTH OF PERSONAL INFORMATION ITS RECORDS CONTAIN¹



REPORTABLE HIPAA VIOLATIONS CAN COST U.S. HEALTHCARE ORGANIZATIONS \$50,000 PER INCIDENT, UP TO \$1.5 MILLION PER YEAR. CRIMINAL IMPRISONMENT PENALTIES CAN RANGE FROM 1 TO 10 YEARS.²

INTUITIVE AUTHENTICATION TO IMPROVE PRODUCTIVITY AND COMPLIANCE

MULTIFACTOR AUTHENTICATION EXPONENTIALLY INCREASES SECURITY

Synchronoss Universal ID makes this critical capability user friendly by enabling users to leverage their own devices to authenticate, such as smartphones, tablets, or other computers.

Key features:

- Online and inherited identity proofing
- Issuance of identity and digital signing credentials
- Secure, multifactor authentication
- End-user profile and credential self-service
- Flexible passcode delivery options
- High-availability cloud-based infrastructure
- Out-of-the-box configurations for popular VPN applications
- High-value mobility services like digital signing and approval as a service
- Numerous user preferences for one-time passcode (OTP) delivery method

IDENTITY VERIFICATION: SELF-SERVICE CONVENIENCE

Synchronoss Universal ID features online, easy-to-use, self-service identity verification and digital audit trails to improve productivity while still ensuring security for healthcare organizations and stakeholders, regardless of size or complexity.

Key features:

- Support for automated online knowledge-based assessments
- Support for self-service notary via secure e-fax
- Administrative dashboard for tracking use



SECURE DIGITAL SIGNATURES MADE SIMPLE

The digital signature on a document—e-prescriptions, W-9 form, or internal corporate document—is legally recognized as a “wet” signature. This makes prescription verification and other document-signing duties far more efficient, especially when a provider is out of the office, and makes it infinitely more secure than a printed—and forgeable—handwritten signature thanks to Synchronoss Universal ID identity proofing, credentialing, and multifactor authentication.

Once users have been identity proofed through Universal ID, credentialed, and issued a DEA-compliant digital signing certificate, they’re ready to digitally sign documents quickly and securely.

With a verified digital signature, electronic prescriptions can be sent to the patient’s pharmacy of choice, requiring a patient only to pick up the filled prescription. And for the authorized caregiver, no further action is required once the electronic script is submitted; the caregiver receives a confirmation and it’s recorded in the patient’s record.

Digital signatures can also be used to sign pages in electronic lab notebooks, which could be vital in patent defense. Enterprise users can also apply digital signatures to essential corporate documents, such as employment, financial, or other materials.

Key features:

- Helps healthcare organizations meet Title 21 CFR Part 11 requirements
- Enables pharmacies to comply with DEA Electronic Prescriptions for Controlled Substances (EPCS) rules
- Offers streamlined digital signature interface for end users
- Provides EU-qualified certificates used for authentication and digital signing



ADDRESS COMPLIANCE REQUIREMENTS

- FICAM Level 3 certification
- HIPAA audited and compliant
- DEA CFR-1311-compliant e-prescribing for controlled substances
- FDA Title CFR-21 Part 11 for digital signature guidelines for submitting electronic records
- Cross-certified Federal Bridge Certification Authority (FBCA)
- Federal meaningful-use requirements contained in the 2009 HITECH Act

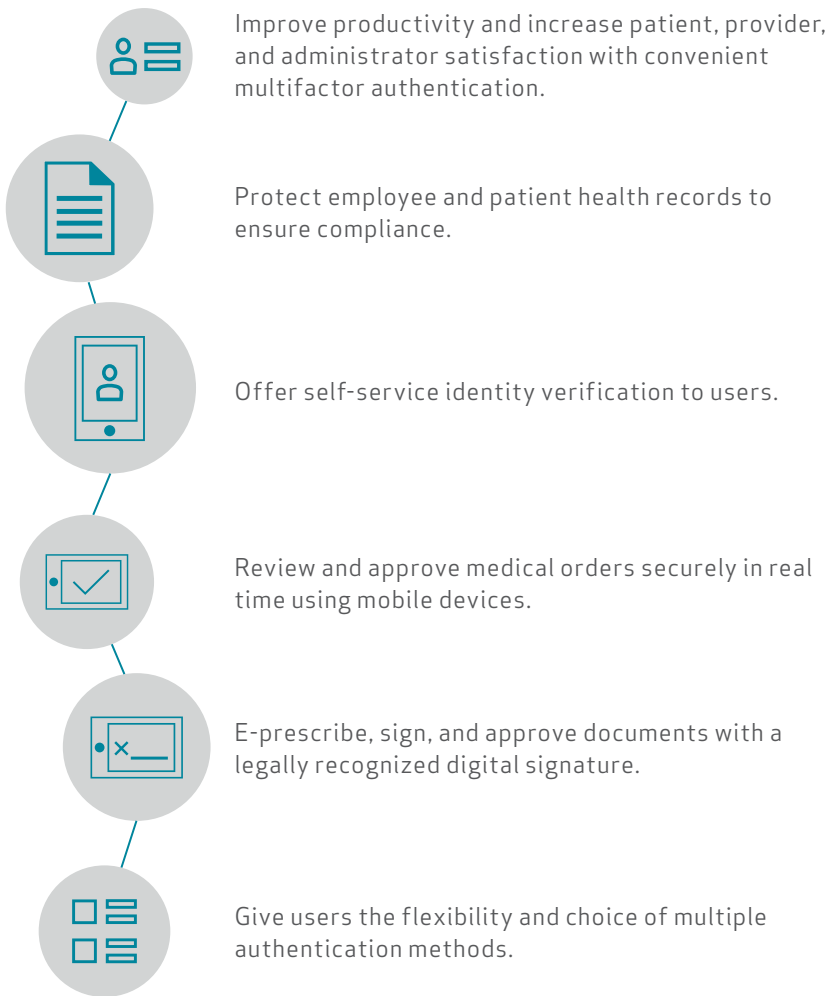
SYNCHRONOSS UNIVERSAL ID MOBILE APPLICATION AND ID MESSAGE CENTER

E-PRESCRIBING AND TRANSACTION APPROVAL

With the Synchronoss Universal ID mobile application and ID Message Center, authorized healthcare stakeholders can access and approve transactions from virtually anywhere, anytime. Healthcare organizations can also choose to implement a web-based version of the ID Message Center using Universal ID. This allows organizations to eliminate time-consuming approvals by allowing instant access to pending, new, or previously approved or rejected transactions—improving efficiency and creating a digital audit trail.

PER-RECORD COST OF HEALTHCARE DATA BREACHES IS \$363, THE HIGHEST OF ALL INDUSTRIES³

HEALTHCARE USE CASES



Synchronoss (NASDAQ: SNCR) is the leader in mobile cloud innovation delivering security, mobility, identity, and analytic solutions for enterprises, mobile carriers, and retailers around the globe. Synchronoss enterprise solutions enable employee productivity without compromising security, allowing enterprises to realize the true power of mobility. For more information, visit us at www.synchronoss.com/identity.

REALIZE THE PROMISE OF ENTERPRISE MOBILITY

Uncompromised productivity and security. Our Secure Mobility Platform meets today's needs and can help make tomorrow's possibilities a reality. It is designed to enhance and complement existing mobility investments, so you get a better ROI—and can finally realize the true power of mobility.

Synchronoss Enterprise delivers real mobility for enterprises with the most stringent security requirements. The Secure Mobility Platform enables highly regulated businesses to build toward modern mobility in a way that complements existing investments.

Synchronoss Enterprise, in a joint venture with Goldman Sachs and Verizon, is extending deeper into the enterprise to bridge the gap and solve the inherent complexity associated with mobility and identity.

Since 2000, we've provided cloud solutions and software-based activation to communication service providers across the globe. Companies such as AT&T, Verizon Wireless, Comcast, Time Warner Cable, Apple, and Microsoft have used our scalable technology solutions to allow their customers to connect, synchronize, and activate connected devices and services that power the connected world.

We know mobility. We know security. We can help your organization do secure business—everywhere.

1. *Hackers, Phishers, and Disappearing Thumb Drives: Lessons Learned from Major Health Care Data Breaches*, Center for Technology Innovation at Brookings, May 5, 2016.
2. "Enforcement and Penalties for Noncompliance," *Summary of the HIPAA Privacy Rule*, U.S. Department of Health & Human Services, 2003.
3. Ponemon Institute, *2015 Cost of Data Breach Study: United States*, IBM Security, May 2015.