AllClear CrossChannel™ Platform

No Contact, No Friction Patient Access

Mobile technology and apps have fundamentally changed what qualifies as a friction-free experience. Patients are sold on the mobile app conveniences they observe in other industries and are becoming intolerant of journeys with too much friction. This includes requiring passwords to access online patient portals, providing personally identifiable information every time they check in, and using pen and paper to sign forms and authorize consents.

Health care organizations with a mobile-first strategy are taking full advantage of the powerful devices their patients carry 24/7 while health systems that operate online patient portals and in-person clipboard check-in experiences are stuck with the old ways of doing things.

Meanwhile, cybersecurity threats and security regulations compound friction in every channel—including mobile. Recently, the Federal Trade Commission issued a warning regarding a noticeable uptick in identity fraud now that more people are interacting via less-than-secure electronic methods. More people are working from a home office, accessing health care services via un-proven mobile apps and clicking on "urgent" text messages and emails that may or may not originate from trusted sources. Even health care organizations with mature mobile applications are forced to restrict their functionality because they can't fully trust the patient's device.

Health care organizations are caught in a vice with friction intolerance on one arm and security concerns on the other. Patients are left wondering why they can't use their mobile devices to do more transactions with their health care providers, especially during this time of physical distancing when remote interaction is the preferred means of doing business.

Savvy health systems are responding by transforming their mobile app into a cross-channel tool that removes obstacles and unleashes innovation no matter where, how or when their patients engage.

For example:

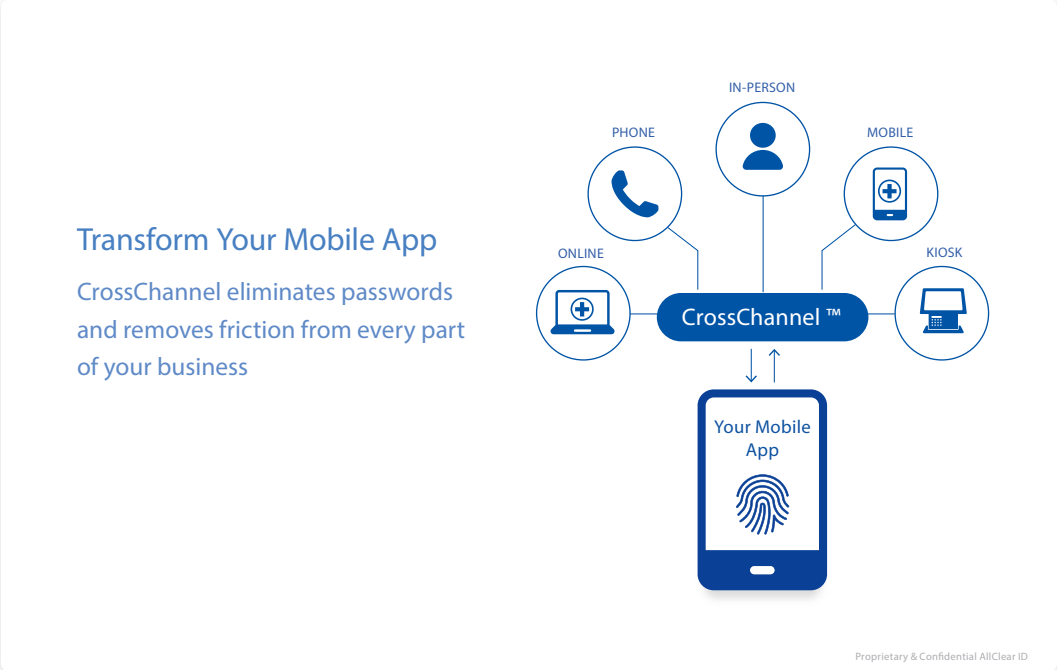
- Instead of relying on passwords and security questions, health care organizations are inviting patients to use their mobile app to access patient portal and telehealth services with the touch of a finger. They are eliminating passwords entirely—not simply using biometrics to autofill passwords on the device.
- Rather than using email or third-party services to acquire signatures, health care organizations send documents directly to the mobile app for biometric signature.
- Rather than asking patients to use pen and paper to sign in, the mobile app is used to signal the patient's arrival providing a no-touch check-in experience
- Instead of restricting app functionality because of HIPAA security concerns, health care organizations are implementing protections that keep their app safe from mobile threats and man-in-the-middle attacks.
- Instead of an in-person ID validation process, allow the patient to remotely confirm their identity by taking an image of their driver's license and recording a video "selfie" to confirm that the photo on their license matches their face in the video

This white paper describes a transformative platform that makes these experiences possible and highly secure.

Introducing the AllClear CrossChannel™ Platform

CrossChannel is a cloud-based platform that connects your mobile app to every part of your enterprise. The idea is simple. Give patients the convenience, speed and security of mobile and connect it to all patient-facing channels; online, in-person, telehealth, kiosk and mobile. The result is a patient experience that is faster and more secure by design.

ILLUSTRATION 1:



CrossChannel's In-App Automations are the key to bringing mobile technology to every channel.

- **In-App Authentication replaces passwords:** Now patients can use their fingerprint or face on their mobile device to authenticate in every channel. No more passwords or security questions.
- **In-App Signatures eliminate delays:** Rather than using a pen and paper or a signature pad to sign documents, patients can instantly sign documents within your app using their mobile biometrics.
- **In-App Authorization reduces phone calls:** Instead of requiring phone calls, email, faxes or face-to-face interactions to authorize important transactions; enable in-app authorization with context plus biometric authentication and electronic audit trails.
- **In-App Location serves as a risk indicator:** Bring the power of mobile GPS to every channel to confirm the patient's location at the time of the transaction and spot anomalies or outliers that could be an indication of fraud.
- **In-App Security unleashes features:** Banking grade security protects apps from mobile threats so that you can release high value features with confidence.
- **In-App ID Confirmation:** Patients take and submit an image of their driver's license along with a biometric facial image with liveness detection using their mobile device. Rapid receipt and validation of the identity document confirms that the patient is who he claims to be.

Patient Misidentification

- Patient misidentification at the point of registration and check-in commonly leads to the creation of duplicate and overlaid records
- Approximately 9% of patient misidentification cases lead to patient harm[1]
- 10% of patient misidentification occurs during a patient record search[2]
- 35% of denied claims can be attributed to patient misidentification[3]

ILLUSTRATION 2:

[1] http://promos.hcpro.com/pdf/2016-national-report-misidentification-report.pdf
[2] https://www.imprivata.com/blog/patient-misidentification-numbers
[3] https://www.imprivata.com/blog/patient-misidentification-numbers

Patented and Proven

CrossChannel is banking grade technology that accelerates over 345 million financial transactions every year for banks, retailers and health care. The core engine, Encap, is a third-generation product that is highly configurable and runs reliably on over 2 million iOS and Android devices. No scalable attacks have been reported since its introduction in 2012, and the core technology is certified to meet the world's highest banking standard for authentication, Secure Customer Authentication (SCA).

The CrossChannel Platform:

- Radically reduces friction in every part of your business
- Unleashes innovation with In-App Automations
- Increases customer engagement by up to 300%
- Keeps systems safe with proven banking grade security

Health Care Use Cases

The technology limitations in different channels serve up a "friction cocktail" that confounds patients holding superior technology in their hand. In a typical health care journey, a patient goes online to research local physicians and confirm that their insurance is accepted. They then make a phone call to schedule an appointment, get a reminder sent to them on a mobile app and when they arrive, they may check-in using a kiosk in the waiting room and be asked to fill out a set of forms using paper and pen. They sign consent and privacy forms and later they login to their patient portal using a username and password to view their clinical results. Along the way, they have to remember the passwords for each app and website, repeat answers to security questions and sometimes dust off a fax machine to get the job done.

The CrossChannel platform lets patients use the power of their mobile devices to remove all this friction. Following are a few use cases.

Establish Identity Prior to Arrival: A new patient who has scheduled an appointment receives a push notification on her mobile device to assure her identity. This is accomplished in a few minutes by using the phone's camera to take an image of the front and back of the driver's license and a video selfie to compare the photo on her license to the video image to ensure that she is the card-bearer. The data from the validated driver's license auto-populates fields in the patient's record thus reducing opportunities for fat-fingering or misspelling.

Once her ID has been confirmed, she receives another push to complete a brief clinical assessment and to electronically sign the health system's HIPAA Notice of Privacy Practice using Face ID as her biometric signature. PHI,

Patient Identity Theft[4]

- 45% of hospitals report that a case of patient identity theft has harmed their reputation
- Incidents of patient identity theft may lead to the disclosure of sensitive, personal health information to the wrong individual
- 48% of patients report that they will switch caregivers if their identity is stolen
- Patient Identity Assurance
- Know-Your-Patient efforts indicate that gathering and confirming identity documents such as the patient's driver's license is a Patient Access best practice
- Supportive identity evidence such as a health insurance card with the patient's name on it improves confidence that the individual presenting is who they say they are
- Validated identity attributes contribute to better patient record matching results and reduce opportunities for errors. The following data elements are considered best practice for these purposes:
  - Patient legal name
  - Address
  - Date of Birth
  - Gender
  - Phone Number
  - Photo

[4] http://www.medidfraud.org/

captured through the mobile app, arrives securely at the health system's back end system. The electronically signed and timestamped Notice of Privacy comports with audit trail requirements. The pre-visit process saves both the patient and the staff time and confirms the true identity of the patient prior to arrival.

No Contact Check-in upon Arrival: The patient arrives at the clinic for her scheduled appointment. The registrar greets the patient, confirms that she has the health system's new mobile app and asks for her phone number to facilitate the mobile check-in experience. The registrar enters those digits into the Patient Authentication portal designed specifically for this purpose to trigger a push notification directly to her app. The patient receives the push notification and applies facial biometric to strongly confirm her identity. The patient, now successfully checked-in via the mobile app, shows as "arrived" in the health system's back-end system. Simultaneously, the registrar's Patient Authentication portal reveals the patient has successfully authenticated herself and her record appears on the screen. Clipboard, paper and pen were avoided in this process, limiting the patient's exposure to germs. The registrar didn't need to ask the patient multiple questions and manually enter data to retrieve the patient's record.

Health Plan/Call Center Services: A member has a question about a recent EOB and calls the health plan's 1–800 Member Support line. Instead of interrogating the member with security questions, the IVR invites the member to authenticate using his mobile app while waiting on hold. The member enters the mobile number into the health plan's app and instantly receives a push message to authenticate with his fingerprint. The IVR confirms his identity and connects the caller to an agent for service without the need for identity interrogation.

Drive-up Patient Arrival: A patient, instructed by his physician to get a lab test at a temporary drive-up testing facility, drives to the location and using the health system's mobile app indicates his arrival. Geofencing and the mobile device's GPS capabilities confirms he is physically present at the drive-up testing location. Applying the native biometric device capabilities found on his smart phone, he easily authenticates himself using his facial biometric. After entering some details about his current health along with the make/model/color of his car he is instructed to proceed to numbered parking space to receive his test. Using a tablet and the health system's app designed especially for the purpose, the clinician on site, views the patient's record along with the data just provided. The clinician and patient do not need to engage in 1:1 conversation and can limit their exposure to one another.

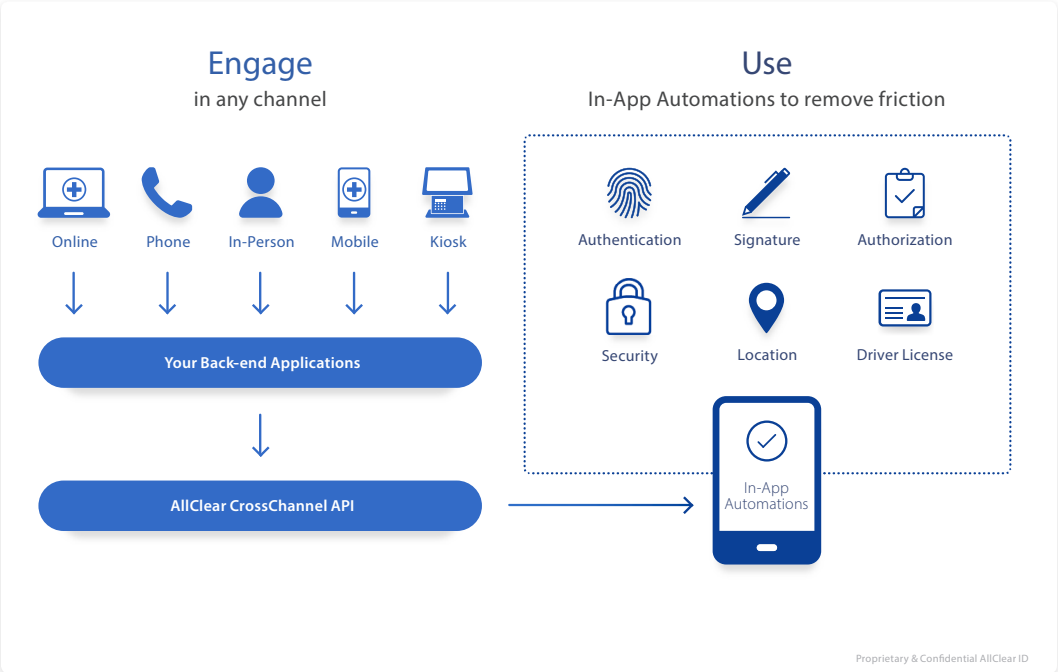
In each of these examples, the patient stays inside the health care enterprise's trusted brand experience with CrossChannel removing friction and securing the patient journey.

How it Works

The CrossChannel solution consists of two components: the CrossChannel API that integrates into back-end applications, and the Mobile Software Development Kit (SDK) that embeds In-App Automations in the mobile app. These components establish a two-way, high security communication channel between the health system's back-end applications and the mobile device. The communication channel is designed to securely transmit any data, images or other personal health information in both directions.

Whenever mobile technology can improve a step in the patient journey, the health system's back-end application pushes the action to the patient's device to accelerate the process. The push message launches the health care organization's mobile app which presents the context and action to the patient. Upon completion, it returns the result and any requested data to the back-end application.

ILLUSTRATION 3: HOW CROSSCHANNEL WORKS



More Secure by Design

The CrossChannel technology was originally designed for mobile-first banks in the Nordics. The central challenge was to safely execute any banking operation on mobile devices and computers that the banks could neither control nor trust. The mobile app was the key, and it needed to be protected even when operating on a compromised platform. The resulting design has proven highly resistant to phishing, malware, man-in-the-middle and other malicious attacks that plague other systems.

First, the design "short circuits" attacks on front-end applications by crossing channels to complete steps using the patient's mobile device. To succeed, attackers must steal the mobile device and overcome multiple security factors (physical device, fingerprint, face, PIN and location). It blocks the front-end attacks that plague password-based systems including:

- Password Theft and Re-use
- Social Engineering
- Friendly Fraud (via non-repudiation)

Second, it blocks man-in-the-middle attacks with forward-secret cryptography that dynamically generates keys within the Trusted Platform Module (TPM) on the device. The TPM is an isolated hardware component designed to keep cryptographic operations secure even when the operating system kernel is compromised.

Third, the CrossChannel Protocol and Mobile SDK combine to block mobile attacks including:

- Device Cloning
- SIM Swapping
- Mobile Malware
- App Debugging
- App Repackaging
- App Emulation

The core technology is certified to meet the world's highest banking standard for authentication, Secure Customer Authentication (SCA). This new standard is defined under Payment Services Directive 2 (PSD2), and no longer permits multi-factor authentication solutions like texting one-time passcodes.

Conclusion:

Mobile technologies have reduced the amount of friction that patients will tolerate, and the technologies used to conduct business in other channels seem antiquated by comparison. Separately, security requirements are compounding friction and forcing health care organizations to limit functionality in every channel.

The AllClear CrossChannel platform addresses this dilemma by transforming mobile apps into cross-channel tools that remove obstacles from every part of a business. This innovative approach has been proven in Nordic countries (see history below) where mobile banking apps are fully functional and highly secure. Now CrossChannel is making this technology accessible and affordable for every industry.

The History Behind CrossChannel

Nordic countries have long been leaders in mobile technology and digital identity solutions. They built the world's most widely adopted digital identity ecosystem used daily by 21 million people to access accounts, make payments and engage government services. The root of this identity design began in 1999 with Norway's BankID scheme that used physical tokens such as key fobs for banking customer authentication.

Sweden began laying plans for their e-ID scheme in 2001, also deploying physical identity tokens. Denmark and Finland soon followed suit, and now all four countries utilize a banking identification scheme that ensures strong consumer identity. Over the past few years, all have matured and strengthened their original authentication designs moving from key fobs to the use of SIM cards to now deploying state-of-the-art app-based solutions using the customers preferred hardware, mobile devices.

Leading the app-based research was Encap AS which started inside the Bank ID project. Encap was eventually spun out to develop a commercial product, and in 2016, Encap and Bank ID demonstrated the convenience and security of the app-based model. Now the entire ecosystem is moving to the app-based model. In 2016 AllClear ID acquired Encap and continued advancing the technology to solve friction problems well beyond authentication. In late 2019, AllClear ID released a SaaS version of the product named CrossChannel. It is powered by the Encap engine, and its purpose is to make this powerful technology accessible and affordable to every industry around the world.

About AllClear ID

AllClear ID, Inc. pioneered the cross-channel technology that allows application builders to use the power of mobile devices to radically reduce friction in any part of their business. The core engine, Encap, features banking grade technology that accelerates over 345 million financial transactions every year for banks, retailers and airlines. It is a proven, third-generation product that is certified to meet the world's highest authentication standard, Secure Customer Authentication (SCA).

The award winning AllClear ID team is also recognized for its identity protection products, high quality service and successful deployment of large-scale managed services. AllClear helped organizations like Anthem Blue Cross, Home Depot and Sony to respond successfully to data breaches affecting 200 million customers. Experian acquired the breach response business from AllClear ID in March of 2019, and the company is now focused exclusively on the CrossChannel/Encap product line.

For more information about AllClear ID and AllClear CrossChannel solution

contact: www.allclearid.com or call 1.877.441.3007