



**Shufti Pro**

Identity Verification



# Know Your Patient

A 360° view of patient  
identification in healthcare

# What's Inside

---

<b>Healthcare industry - An Overview</b>	<b>03</b>
<b>Key stakeholders of the Healthcare industry</b>	<b>04</b>
<b>What is KYP?</b>	<b>05</b>
<b>Key regulations related to patient verification</b>	<b>06</b>
HIPAA - USA	07
HITECH - USA	07
NHS guidance - England	08
GPHC's guidance - UK	08
<b>Applications of KYP</b>	<b>09</b>
Counter medical identity fraud	09
Reducing medical frauds happening due to data breaches	11
Sharing personal healthcare information	13
Improve registration process efficiency	13
Better address verification	14
Protection against identity theft	15

<b>Shufti Pro's KYP for Medical Fraud Prevention</b>	<b>16</b>
Counter medical identity fraud	17
Ongoing KYP using biometric authentication	18
Benefits of KYP Verification	18

# Healthcare industry - An Overview

Healthcare is one of the fastest-growing industries around the world. WHO reported that 10% (7.2 trillion US dollars) of global GDP was spent on healthcare in 2015<sup>[1]</sup>. While global healthcare spending is expected to reach \$10.59 trillion by 2022. Healthcare is evolving from patient care, medications, to technically evolved traditional medicare operations. No-cut surgical techniques and robotic healthcare is the new norm. On the other hand, pharmaceuticals are utilizing real patient data to conduct extensive research for the invention of next-generation medicines. The allied industries of healthcare such as insurance companies, medicine suppliers, and patient verification companies are shaping the future of healthcare operations with state of the art technologies that further enhances the operational efficiency of the industry.

Care providers, product manufacturers, pharmaceuticals and several stakeholders of the health economy use patient data for security, research, regulatory compliance, fraud prevention, patient verification and several other purposes. But using patient data is not as simple as it may sound, Personal Health Information (PHI) used in these industries is to be handled with diligence. Nearly 53% of global healthcare organizations experienced a cyber attack in the last 12 months (keeper security)<sup>[2]</sup>. Increasing data breaches exposes patients and healthcare providers to gigantic risks of financial loss, defamation, and health hazards to name a few. This is why KYP (Know Your Patient), PHI, and medication laws are implemented all over the world.

[1] Health Financing

[2] 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses

# Key stakeholders of the Healthcare industry

Stakeholder			Access to Patient information		
	Purpose	Types	PHI (Personal Health Information)	Identity information	Insurance (payment) details
Healthcare services and facility	Generally involved in providing healthcare services	<b>Hospitals</b> Emergency care providers, Dental laboratories, Psychiatric hospitals, etc	Yes	Yes	Yes
		<b>Facilities</b> Nursing care facilities, In-home care, Rehabilitation centres, etc	Yes	Yes	Yes
		<b>Practitioners</b> Social workers, therapists, dietitians, etc	Yes	Yes	Yes
Pharmaceutical	Works on medicine manufacturing, sales, and marketing.	<b>Sellers</b> Over-the-counter (OTC) drug stores, Home delivery drug stores, online drug stores	Yes	Yes	No
		<b>Manufacturers</b> Drug manufacturing companies, etc	Yes (for research purposes)	Yes	No
Allied industries	<b>Insurance</b> Provides medical insurance	Life/accident/health insurance companies, Corporate health insurance companies, etc	Yes	Yes	Yes
	<b>Collection management</b> Provides bills collection services to healthcare providers	Bills collection services, Patient eligibility analysis services, Benefits management services, etc	Yes	Yes	Yes
	<b>Patient verification</b> Verifies patient identities for all the above-mentioned healthcare stakeholders	Know your patient verification companies, Patient address verification services, online patient verification companies, Biometric patient authentication services providers	Yes (if the healthcare provider needs them to verify this information)	Yes	Sometimes

## | What is KYP?

KYP (Know Your Patient) is the term used for patient verification according to the state laws and patient identification policies of the hospital. Patients are verified from their government-issued identity documents, insurance documents, and/or hospital-issued ID cards. It's pretty much the same as the KYC (Know Your Customer) processes in banking and other industries. Patient verification is a vital part of healthcare and its allied industries conducted to achieve goals such as:

- to prevent medical identity fraud
- for responsible selling of prescription-only drugs
- to deliver better online patient care
- to comply with patient care regulations
- to deliver better healthcare
- to maintain updated patient data

Healthcare organizations use personal health information and identity details of patients to deliver better services. A patient shares his data with more than one stakeholders for getting a single treatment. This data is collected and verified to fulfil multiple reasons mentioned above and in accordance with laws such as HIPAA, HITECH, CLIA, etc.

The next section will describe the patient verification laws practices in developed nations.

## Key regulations related to patient verification

Patient authentication is a significant part of patient identification policies at healthcare organizations.



Below is a list of laws that are implemented on care providers in different regions across the globe.

## HIPAA (Health Insurance Portability and Accountability Act - 1996) - USA

This act has five rules namely privacy rule, transaction and code set rule, security rule, employer identifier rule and enforcement rule. The privacy rule requires the covered entities to establish written policies designed to verify the identity and authenticity of the person requesting the Protected Health Information (PHI). This rule highlights the regulatory requirements of due diligence that need to be practised if PHI is disclosed to individuals known or not known to the healthcare provider. (Source: ASPE)<sup>[3]</sup>

These regulations can be met in an electronic information sharing environment. Documents required for disclosure can be shared electronically in the form of scanned images or pdf files. (Source: HHS)<sup>[4]</sup>

## HITECH (Health Information Technology for Economic and Clinical Health Act - 2009) - USA

This act was introduced to encourage hospitals to adopt EHRs (Electronic Health Records). The Act increased the rate of adoption of EHRs from 3.2% in 2008 to 14.2% in 2015. By 2017, 86% of office-based physicians had adopted an EHR and 96% of non-federal acute care hospitals had implemented certified health IT. This act also applied tougher penalties for violations with HIPPA law. (Source: HIPAA Journal)<sup>[5]</sup>

<sup>[3]</sup> Disclosure of Protected Health Information

<sup>[5]</sup> HIPAA Journal

<sup>[4]</sup> HHS

## NHS guidance - England

NHS Good Practices Guidance provides guidelines to the general practices for verification of patients and their representatives when extending online services. This guideline provides three identity verification methods, guidelines on authorization, record keeping, identity verification process details and much more. (Source: NHS guidance)<sup>[6]</sup>

## GPHC's guidance for pharmacies providing services at a distance - the UK

GPHC's guidance provides guidelines for the pharmacies that provide remote services. Types of pharmacies covered include collection and delivery, click and collect, and hub and spoke. The principal 4 guides the covered entities to verify the identity of the patient through appropriate checks before selling drugs to them. Even if a pharmacy is providing medicines to an intermediary and not to the patient directly, they must ensure that the intermediary has comprehensive patient verification procedures in place. (Source: GPHC - Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet)<sup>[7]</sup>

<sup>[6]</sup> NHS guidance

<sup>[7]</sup> GPHC's guidance

# Applications of KYP

Now that you know what KYP is let's explore how it is relevant to several industries and why it's crucial for better healthcare. Under current law, national health spending is projected to grow at an average rate of 5.5% per year for 2018-27 and to reach nearly \$6.0 trillion by 2027 (Source: CMS.gov<sup>[8]</sup>).

Patient verification is crucial for the healthcare industry and it's allied industries and serves multiple use cases, a few of them are discussed below:

## 1. Counter medical identity fraud

There were 3,054 healthcare data breaches involving more than 500 records, during 2009 - 2019, causing loss, theft, exposure, and impermissible disclosure of 230,954,151 healthcare records (Source: HIPAA Journal<sup>[9]</sup>). Medical identity fraud affects care providers, insurance companies, pharmaceuticals and patients equally. Sometimes the consequences of fraud might not only result in lost insurance benefits or penalties but also put the life of original patients at stake.

Medical identity is stolen by criminals, patients, minors, drug dealers and even doctors. An Orchard Park pain management doctor pleaded guilty of using patient identities to get controlled

[8] CMS.gov

[9] Healthcare Data Breach Statistics

substances. He wrote multiple prescriptions with names and date of births of his two deceased patients. The medicines were shipped to his home or office (medical marijuana practice), by a pharmacy and consumed by the doctor himself. Such charges of medical identity theft carry a maximum penalty of five years in prison (Source: DEA)<sup>[10]</sup>.

*“Health care fraud affects all Americans because it increases the cost of health insurance and reduces the amount of money insurance plans have available to pay legitimate claims,” said U.S. Attorney Billy J. Williams<sup>[11]</sup>*

Stolen medical data is commonly used to get the health benefits of the victim or to make fraudulent insurance claims at health care organizations, health facilities and insurance providers. A Pittsburgh resident pleaded guilty of health fraud, aggravated identity theft and conspiracy in March 2020. She admitted committing identity fraud to make fraudulent claims for obtaining millions of dollars through the Pennsylvania Medicaid program. She submitted claims for home services that she never provided and on behalf of ghost employees (Source: United states department of justice - news)<sup>[12]</sup>.

Medical fraud happens in a variety of ways and could be due to negligence on behalf of hospitals, patients, insurance companies and even government authorities. Verification of patient identifiers and medication identifiers at multiple stages of health care is crucial to deliver better healthcare to deserving people and to control the soaring costs of healthcare.

[10] DEA (Drug Enforcement Administration)

[12] Health Care Fraud and Aggravated Identity Theft

[11] Springfield Woman Sentenced to Prison for Health Care Fraud

## 2. Reducing medical frauds happening due to data breaches

Several medical data breaches happened in the last few years exposing millions of medical records. A report by Protenus stated that over 41M patient records were exposed during 2019 in 481 incidents reported to the US Department of Health and Human Services (HHS) (Source: Protenus)<sup>[13]</sup>. These stolen credentials are sold for at high prices ranging from \$70 to \$ 100 on the dark web and used to conduct million dollar crimes (Source: total processing)<sup>[14]</sup>. These data breaches affect not only the healthcare industry but it's allied industries including but not limited to insurance companies, government organizations, pharmaceuticals, and medical facilities.

A 2019 Carbon black report on healthcare organizations found that 83% of the surveyed organizations have seen an increase in cyber frauds in the past year<sup>[15]</sup>. Similarly, healthcare data online is also vulnerable to cyberattacks<sup>[15]</sup>.

**Paul Katzoff, CEO of WhiteCanyon Software emphasized on reducing the number of data breaches.**<sup>[16]</sup>

“Identity Thieves purchase sensitive personal information (SPI) on the black market (Dark Web). There is a whole economy of bad actors working to secure your SPI, sell that SPI, purchase the SPI and use the SPI for fraudulent transactions. Verified Credit Card details can be purchased for \$1-\$2 per record.

<sup>[13]</sup> 2020 Breach Barometer

<sup>[15]</sup> Carbon Black Threat Report

<sup>[14]</sup> How Much is your Data Worth on the Dark Web?

<sup>[16]</sup> WhiteCanyon Software

Health insurance details go for a lot more ~\$100 per record. Health insurance information is a big concern right now. Perpetrators get your health insurance information, get a fake ID and go in and see a Dr about hip/knee replacement surgery. The Dr does the evaluation, recommends surgery and surgery gets scheduled.

The perpetrator will then go in, get the surgery done and leave the hospital. The victim will receive a letter 30 days later with the statement of the surgery and their out of pocket costs. The victim has no idea about the surgery and has to report the fraud. By then the perpetrator is long gone.” Paul Katzoff



### 3. Sharing personal healthcare information

Healthcare service providers share personal healthcare information with several stakeholders such as doctors, healthcare facilities, patients and their guardians, insurance firms, government organizations, etc.

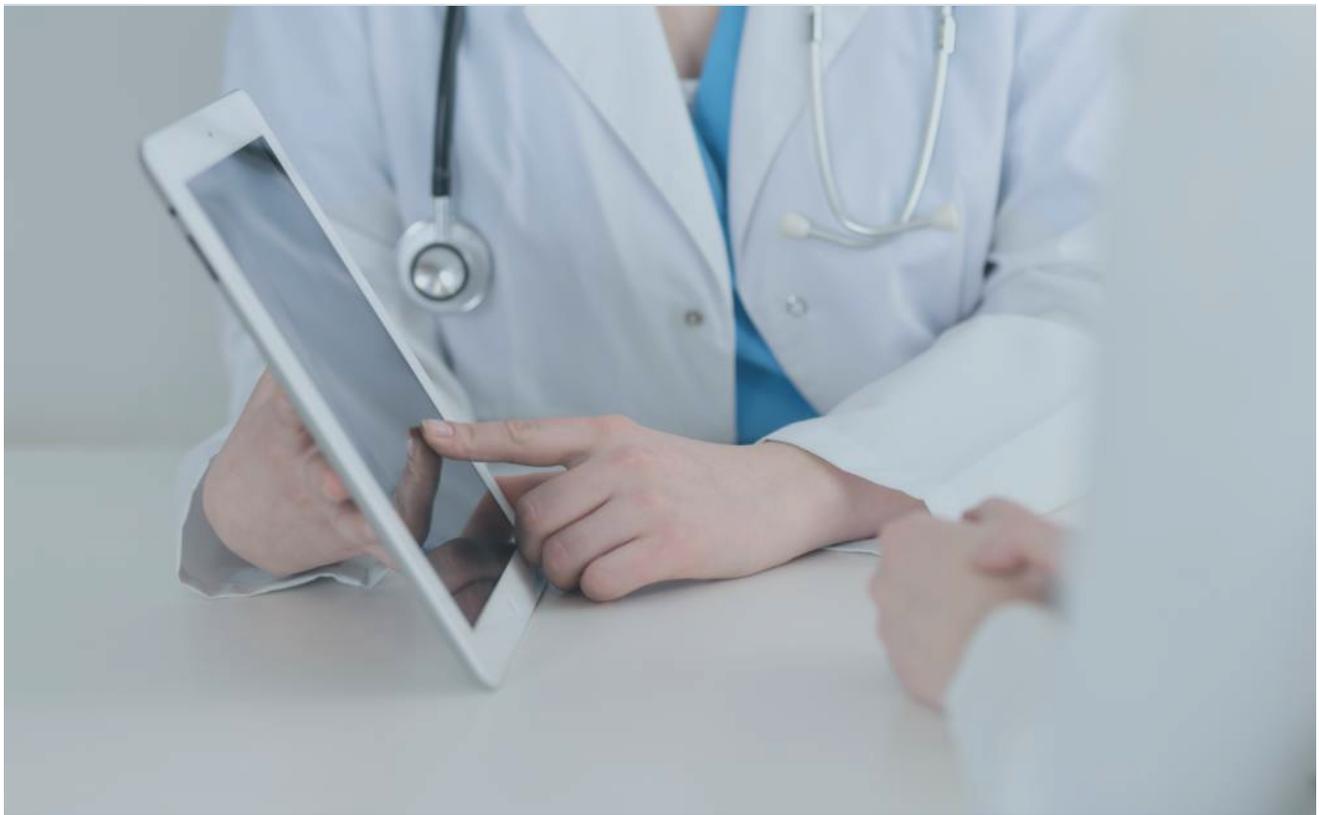
Manual sharing is prone to errors and increases cyber risk. With the advent of telehealth, it is becoming increasingly crucial for healthcare providers to maintain secure digital records of their patients. Not only does it improve the quality of services but ensures safe data sharing.

### 4. Improve registration process efficiency

Traditional registration and onboarding processes require a lot of time and manual work. Customers had to go through a lengthy onboarding process and in some cases had to wait for days to get their identity verified. While customer experience isn't the only problem in manual onboarding, medical service providers also have to perform laborious tasks to verify the identity and manage a huge amount of physical data. Also, this manual process could result in errors resulting in the financial and reputational loss.

AI-based automated verification, on the other hand, is free from these kinds of errors and doesn't involve a lot of manual work. It enhances the efficiency of the registration process by reducing manual work and managing data securely. Apart from this, these

technologies can easily be integrated with online platforms reducing the registration cost to a minimal level.



## 5. Better address verification

With the emergence of telehealth, many people are adopting online medical purchasing habits. There are, however, some risks involved when selling medicines online. One of these risks is chargeback claims. With increasing online purchasing the chances for chargebacks and wrong deliveries increases for the online medicine selling platforms. And if not overcome these chargebacks could lead to fines and penalties.

Address verification of the customer is one way of minimising these issues. If the address of a customer is verified at the time of registration and checkout the chargeback and misplaced deliveries will be minimised.

## 6. Protection against identity theft

Identity theft in the healthcare sector is a growing problem. In fact, 27% of the data breaches in 2017 were related to medical records.<sup>[17]</sup> Additionally, 30% of the victims had no idea when the identity theft occurred. Medical identity theft is nothing new, the more advanced technology grows, more sophisticated medical identity frauds become.

However, with the help of right technology medical identity frauds could be stopped just like in any other industry. With the right technology to verify the identity of patients, identity theft cases could easily be put to a halt. Even if fraudsters are able to get someone's identity data on the black market they won't be able to use these records if ongoing patient verification checks are in place. This will not only help healthcare businesses in securing their platform but also serve as a bigger purpose of maintaining the integrity of the healthcare sector.

# Shufti Pro's KYP for Medical Fraud Prevention

Owing to the increasing emphasis on online healthcare solutions especially after COVID-19 pandemic, Shufti Pro - a keen believer of creating secure online marketplaces decided to provide identity verification services to the healthcare organisations. Going forward, the regulations for medical facilities will become more stringent as the COVID-19 related scams have highlighted the importance of fraud prevention checks for online businesses. Shufti Pro's KYP verification solution is a tool against cybercrimes, especially medical identity fraud, that results in data breaches.



Using AI-based verification technology, Shufti Pro makes customer identification more secure and accurate.

## How does KYP verification work?

For online identity verification of people registering on a hospital's portal, opening an account on medical health insurance platforms or trying to purchase medical drugs from online stores, the businesses need to simply integrate Shufti Pro's KYP solution into their platform<sup>[18]</sup> for online identity and age verification. Once integrated, the patient can be verified through his/her identity document by following these simple steps:

-  The individual needs to take a selfie of their face along with their identity document.
-  The AI-based verification system detects and extracts the information from the ID document and matches it with the one provided in the form.
-  Biometric authentication is performed via liveness detection and 3D depth perception to conduct face verification.
-  The age verification of the patient is also performed after verifying the date of birth from the identity document.

## Ongoing KYP using biometric authentication

Once the user verification is initially accepted/rejected, pharmacies and clinics can perform further authentication with a simple selfie. The process is easy; at the time of initial screening, a live 3D face map of the user is created using facial recognition technology and every time a user wants to authenticate the transaction it can be done with a single selfie. The selfie of the user is matched with a face map captured during the initial screening.

## Benefits of KYP Verification

- Identity verification of the remote patients becomes easy for medical services
- Responsible selling by secure patient identification for online pharmacies
- Enhanced KYC compliance for on-premise and online medical services
- Ongoing patient authentication for continuous fraud prevention
- Accurate verification through govt-issued ID cards for fighting insurance frauds

# Integrate enhanced security solution to prevent fraud and fulfil KYC regulations

Try Now

Contact Us

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

✉ [sales@shuftipro.com](mailto:sales@shuftipro.com)



Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from [3000+ ID](#) templates and business entities from [200 million](#) companies data.

**Disclaimer:** No warranty or claim is herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute as legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.