Biometrics and Healthcare

This report examines how biometric technology is applied to the health care industry, mainly in the United States. This report notes that "health care biometrics" is utilized for access control, identification, workforce management or patient record storage. Biometrics in health care often takes two forms: providing access control to resources and patient identification solutions. The growing demand for biometrics solutions is mainly driven by the need to combat fraud, along with the imperative to improve patient privacy along with health care safety. Biometrics are also increasing being used for medical monitoring and mobile health care.

Rawlson O`Neil King
Lead Researcher, Biometrics Research Group, Inc.

Healthcare Providers Say Yes to Fingerprint Authentication

No More Passwords

Leading hospitals and clinics along with group and private medical practices are witnessing the benefits of fingerprint authentication.

Eliminate Passwords, Tokens, Cards and PIN's

Achieve Complaint Two-Factor Authentication

Enhance Current Workflow Processes

Increase Time to Care for Patients

BIO-key International, Inc.

www.bio-key.com | 866-846-2594

BIO-key™

Revolutionizing Authentication

TABLE OF CONTENTS

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

Introduction

Biometrics for the health care industry primarily refers to staff authentication and patient identification solutions. Most often, biometrics are used in combination with passwords or smart identification cards to secure access to sensitive patient records and to assist with patient registration requirements. Biometrics Research Group, Inc. estimates that the entire global marketplace for biometric solutions in the health care market will reach approximately US$5 billion by 2020. Biometric use will reflect the growing demand for health care fraud prevention in the United States, along with the need to improve patient privacy and health care safety.

1. Health care in the United States

Health care is one of the most important expenditure categories within the U.S. economy. According to the World Health Organization (WHO), total health care spending in the U.S. was 17.9 percent of its gross domestic product (GDP) in 2011, the highest in the world. The Health and Human Services Department expects that the health share of GDP will continue its historical upward trend, reaching 19.5 percent of GDP by 2017.

In 2013, U.S. health care spending reached US$2.9 trillion, or US$9,255 per person and generated billions of claims from millions of health care service and product providers. Medicare alone represents 47 million beneficiaries, which pays over 4.4 million claims each working day through 1.5 million providers.

In 2013, households accounted for the largest share of health care spending (28 percent), followed by the federal government (26 percent), private businesses (21 percent), and state and local governments (17 percent). Of each dollar spent on health care in the United States, it is estimated that 31 percent is allocated to hospital care, 21 percent is allocated to physician and clinical services, 10 percent is allocated to medication, four percent to dental, six percent to nursing homes and three percent to home health care. In addition, three percent is allocated to other retail products, three percent to government public health activities, seven percent to administrative costs, seven percent to investment, and six percent to other professional services, such as physical therapists and optometrists. Despite high levels of spending on health care, relative to other industrialized countries, most analysts rank the United States last in the quality of care provided, on the basis of economic investment versus actual health outcomes.

Reasons are myriad for poor performance when compared to high levels of investment. The health care system in the United States has traditionally been bifurcated between those who have insurance and those who do not. Unlike other industrial nations, the United States has not adopted a singular, national health care system provided by public insurance, funded through taxation. Instead, health care provision is fragmented between an inefficient mix of public and private insurance.

Health care facilities are largely owned and operated by private sector businesses. Health insurance for public sector employees is primarily provided by the government. It is estimated that approximately 65 percent of health care provision and spending comes from government programs, including Medicare, Medicaid, TRICARE, the Children's Health Insurance Program, and the Veterans Health Administration. However, most of the population under 65 is insured by a family member's employer, or under a privately-purchased health insurance policy. The remainder are uninsured.

Table 1 - U.S. Government Health care Programs

Medicare	Medicare is a national social insurance program, administered by the U.S. federal government since 1966, currently using about 30 private insurance companies across the United States. Medicare provides health insurance for Americans aged 65 and older who have worked and paid into the system. It also provides health insurance to younger people with disabilities, end stage renal disease and amyotrophic lateral sclerosis.
Medicaid	Medicaid in the United States is a social health care program for families and individuals with low income and limited resources. Medicaid has been described as a government insurance program for persons of all ages whose income and resources are insufficient to pay for health care.
TRICARE	TRICARE is a health care program of the United States Department of Defense Military Health System. TRICARE provides civilian health benefits for military personnel, military retirees, and their dependents, including some members of the Reserve Component of the United States Armed Forces. TRICARE was formerly known as the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS).
Children's Health Insurance Program	Children's Health Insurance Program (CHIP) is a program administered by the United States Department of Health and Human Services that provides matching funds to states for health insurance to families with children. The program is designed to cover uninsured children in families with incomes that are modest but too high to qualify for Medicaid.
Veterans Health Administration	Veterans Health Administration (VHA) is the component of the United States Department of Veterans Affairs (VA) led by the Under Secretary of Veterans Affairs for Health that implements the medical assistance program of the VA through the administration and operation of numerous VA Medical Centers (VAMC), Outpatient Clinics (OPC), Community Based Outpatient Clinics (CBOC), and VA Community Living Centers (VA Nursing Home) Programs.

Around 84.7 percent of Americans have some form of health insurance; either through their employer or the employer of their spouse or parent (59.3 percent); purchased individually (8.9 percent); or provided by government programs (27.8 percent; there is some overlap in these figures). All government health care programs have restricted eligibility, and there is no one government health insurance policy that covers all Americans. Americans without health insurance coverage in 2007 totaled 15.3 percent of the population, or 45.7 million people.

2. Health care fraud in the United States

Due to the complexity of a fragmented health insurance regime in the United States, the system is highly susceptible to fraud. Health care fraud is a white-collar crime that involves the filing of dishonest healthcare claims in order to turn a profit or to access services illegitimately. Health care fraud has been defined as an intentional deception or misrepresentation that an individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party.

Fraudulent health care schemes come in many forms. In the United States, the most common kind of health care fraud reportedly involves a false statement, misrepresentation or deliberate omission made by a health care recipient that is critical to the determination of benefits payable. Fraudulent activities are almost invariably criminal, although the specific nature or degree of criminal acts vary from state to state.

The degree of health care fraud throughout the United States is such that it is estimated that the amount of money the American health care system loses could pay for insurance for the uninsured, keep premiums from rising and could improve the general health of Americans.

While there are no exact figures on the cost of health care fraud in the United States, estimated annual losses are in the billions of dollars. The FBI estimates that between US$75-$250 billion is lost annually in health care programs nationwide, based on the assumption that fraudulent billings to public and private health care programs totals three to 10 percent of total health care expenditures. Other estimates have placed total annual losses to health care fraud at between US$125-$175 billion. The Coalition against Insurance Fraud, an anti-fraud watchdog group consisting of consumers, insurers, legislators and regulators estimates that US$80 billion is lost annually in Medicare fraud alone. According to the National Health Care Anti-Fraud Association, an organization of approximately 100 private insurers and public agencies, US$69 billion is lost annually in all health care programs nationwide (based on 2010 calculations of three percent of national health care spending).

Taxpayers bear the burden of Medicare fraud, waste, and abuse. In addition, the fraud numbers for private health insurance plans, secondary payers, and "Medigap plans," or private insurance policies, are likely to be high as well, though that data is not publicly available.

During the 2011 fiscal year, the Justice Department, working in collaboration with the U.S. Department of Health and Human Services, was able to recover nearly US$4.1 billion in funds stolen or taken improperly from federal health care programs. This reportedly represents the highest amount ever recovered in a single year. However, this record breaking recovery accounts for only less than one percent of the total funds lost through fraud waste and abuse in 2011. A report published by the U.S. Government Accountability Office (GAO) discovered that medical facilities and durable medical equipment providers were the most frequent subjects of criminal fraud cases involving Medicare or Medicaid, with hospitals and medical facilities

cited as the most frequent subjects of civil fraud cases resulting in judgments or settlements. Only 11.1 percent of the cases investigated and prosecuted for health care fraud involved individual citizens as the perpetrators. Typically, fraud schemes are executed by medical practitioners.

Practitioner schemes include: individuals obtaining subsidized or fully-covered prescription medicine that is unneeded and then selling them on the black market for a profit; billing by practitioners for care they never rendered; filing duplicate claims for the same service rendered; altering the dates, description of services, or identities of members or providers; billing for a non-covered service as a covered service; modifying medical records; intentional incorrect reporting of diagnoses or procedures to maximize payment; use of unlicensed staff; accepting or giving kickbacks for member referrals; waiving member co-pays; and prescribing additional or unnecessary treatment.

Individuals can commit healthcare fraud by providing false information when applying for programs or services, forging or selling prescription drugs, using transportation benefits for non-medical related purposes and loaning or using another's insurance card.

Typically, when health care fraud is perpetrated, the provider passes the costs along to its customers. Due to the pervasiveness of healthcare fraud, statistics currently estimate that 10 cents from every dollar spent on health care in the United States goes toward paying for fraudulent health care claims.

Congressional legislation requires that health care insurance pay a legitimate claim within 30 days. The Federal Bureau of Investigation, the U.S. Postal Service, and the Office of the Inspector General all are charged with the responsibility of investigating health care fraud. However, because of the 30-day rule, these agencies rarely have enough time to perform an adequate investigation before an insurer has to pay. A successful prosecution of a health care provider that ends in a conviction can have serious consequences. The health care provider faces incarceration, fines, and possibly losing the right to practice in the medical industry. Violators may be prosecuted under: 18 U.S.C. 1347.

The deleterious effects of health care fraud and system inefficiency are therefore driving the deployment of biometric security solutions in the sector. Biometrics Research Group, Inc. defines biometrics as measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity. Biometric patterns can be anything from fingerprints, iris scans, palm prints, gait, facial recognition or even voice recognition.

Biometrics is the science of recognizing an individual based on his or her physical and behavioural traits. Biometric-based authentication systems are widely considered to be more reliable than established password systems for verifying individuals and ensuring they are who they say they are.

3. Health care Biometrics

Biometrics Research Group, Inc. uses the term "health care biometrics" to refer to biometric applications in doctors' offices, hospitals, or for use in monitoring patients. This can include access control, identification, workforce management or patient record storage. Biometrics in health care often takes two forms: providing access control to resources and patient identification solutions.

Many hospitals and healthcare organizations are currently deploying biometric security architecture. Secure identification is critical in the healthcare system, both to control logical access to centralized archives of digitized patients' data, and

to limit physical access to buildings and hospital wards, and to authenticate medical and social support personnel.

There is also an increasing need to identify patients with a high degree of certainty. Identity verification solutions based on biometric technology can provide identity assurance and authentication, thereby lowering health care fraud instances, while increasing privacy and security. Biometric technology can add operational efficiencies to the healthcare system that reduce costs, reduce fraud, and increase patient satisfaction by reducing medical errors. As electronic health records (EHRs) and personal health records (PHRs) become more commonly used, biometrics are being utilized as an authentication mechanism by both medical facilities and insurers.

Under U.S. federal legislation, specifically the Health Insurance Portability and Accountability Act, records must be kept every time a patient's electronic record is accessed. Biometrics permit medical professionals to do this easily since their use of a biometric identifier can be automatically and digitally recorded each time a medical record is opened. A number of biometric equipment manufacturers and service providers therefore offer turnkey applications that maintain and track access to EHRs.

Such "access to resource" applications include secured authentication protocols for log-in to IT applications in a clinical environment, along with access to modalities and control applications. A benefit of such applications is that they prevent administrative fines and penalties associated with unauthorized access to confidential patient medical information. Such applications also combine high security with convenience and eliminate costly password support by adopting biometric authentication. The use of biometric authentication tools provides the option for health care facilities to extend physical control over access to medicine cabinets and in laboratories. The use of such systems also streamlines workflow by adding sign-off capacity for diagnostic results, patient medication and treatments and for data capture for pharmaceutical trials.

3.1 Workflow Improvement

As an example, BIO-key's fingerprint biometric authentication solutions support the security, workflow and compliance requirements for hospitals and clinics along with group and private medical practices. BIO-key International is a leading provider of fingerprint biometric identification, secure mobile credentialing and user identity verification solutions.

The company recognizes that biometrics are becoming a preferred authentication option that can replace passwords, tokens, cards and PINs and acknowledges that one of the key challenges every health care organization faces is managing the security infrastructure and protecting patient records. Healthcare IT executives are finding that password resets and managing token, card and PIN programs include subtle hidden and recurring costs, which in time, become significant. They also bear intrinsic risk factors such as the ability to be lost, stolen or shared; unlike any biometric solution.

BIO-key's NIST rated software is natively embedded in leading EHR platforms such as EPIC and Allscripts and Single Sign-on providers like HealthCast. BIO-key is also integrated with leading security providers and is offered within the IBM, CA and Oracle security suite. The company's software is interoperable across all devices; fully embracing the bring-your-own-device (BYOD) environment and BIO-key is currently developing the mobile authentication ecosystem for healthcare providers.

In 2006, George Washington University Hospital, became BIO-key's first customer in the healthcare

space. Today, BIO-key fingerprint authentication solutions can be found in thousands of hospitals providing security for McKesson's AcuDoseRx cabinets along with protecting patient records and providing compliant two-factor authentication for EHR platforms. BIO-key future proofs its customers' technology by integrating its software with more than 40 different fingerprint readers; offering a variety of performance and price options for customers.

Recently, one of the world's leading hospitals wanted to improve its existing process for two-factor authentication in order to meet U.S. Drug Enforcement Administration (DEA) and State Board of Pharmacy compliance requirements.

BIO-key's project was specific to the pharmacy department within the hospital, which generated thousands of prescriptions each month. Prior to selecting BIO-key, providers would respond to Challenge Response – Knowledge Based Questions each and every time they wanted to provide two-factor authentication for an electronic prescription.

BIO-key tracked utilization within the department for 30 days. The results were profound. The pharmacy department's staff authenticated 251,447 times during a thirty-day period. Imagine answering the question "What was your first pet's name" a quarter of a million times in a month. BIO-key delivered a 99.34% first-attempt authentication rate. One staff member scored a perfect 5,999 in one touch authentications. This ultimately improved workflow while providing optimum convenience enhancing the overall user experience.

In another example, a well-recognized clinic in Ohio wanted to address workflow challenges within the EHR process. Providers were constantly voicing their displeasure about entering lengthy sophisticated passwords, which were impeding workflow and causing undue stress. The clinic's IT director conducted password resets frequently in an attempt to remain compliant and to enhance security. Yet the ever changing passwords were near impossible to remember, therefore causing staff to write them down and store them in open view.

BIO-key worked together with its integration partner Allscripts to deliver a seamless two-factor authentication solution, enabling the clinics to reduce their reliance on passwords and develop a more efficient streamlined approach to accessing patient records. BIO-key's presence and history position them as a leading provider of biometric authentication and identification solutions in the healthcare market.

3.2 Patient Identification Solutions

Another key use of heath care biometrics is for patient identification solutions. Such solutions allow healthcare organizations such as hospitals and clinics to track clientele. Patient identification solutions can be used for client registration, treatment tracking, walk-through of departments and for scheduling and self-services.

Patient identification solutions can accommodate national and private health insurance cards, ambulant treatment documents, wrist bands and most important biometric identification modalities, including fingerprint and palm-vein recognition.

Biometrics Research Group, Inc. expects that patient identification solutions will quickly be adopted in private clinics in the United States on a small scale. In terms of large-scale adoption, we expect that will happen internationally, as governments in emerging nations such as India and developing nations such as Ghana, adopt biometric technology to grant access to public health care programs.

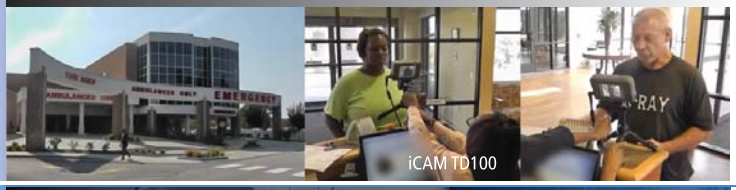
Iris ID Global Leader

IRIS ID
Advanced Identity Authentication™

Best-in-Class Iris Identity Solutions in Healthcare

- Iris ID technology is deployed in leading hospitals and pharmaceutical research facilities.
- Healthcare providers utilize Iris ID technology to enhance security, increase convenience and meet compliance requirements.
- Iris ID IrisAccelerator™ one-to-many matching capability allows healthcare organizations to enroll healthcare providers or patients, and accurately recover their records without requiring any further form of identification.

Patient Enrollment and **Identification**



Patient Enrollment and Identification. Hospitals across the world utilize Iris ID products to accurately identify patients and eliminate insurance fraud.

Photos published with permission from RightPatient®

Access Control and **Workforce Management**

Access Control and Workforce Management. Deployed in hospitals to Secure highly sensitive areas.

Healthcare Solutions

Help protect the Healthcare industry globally. Best performing non-contact biometric.

Iris Recognition Technology from Iris ID

Leading the World of Identity Authentication. Since 1997, Iris ID has been the key developer and driver of the commercialization of iris recognition technology. IrisAccess, now in a fourth generation, is the world's leading deployed iris recognition platform. Found on 6 continents, in thousands of locations, authenticating the identities of millions and millions of persons, more people in more places authenticate with IrisAccess than with all other iris recognition products combined. Some of the programs we have helped make possible are highlighted on this site. Have needs of your own? Talk to us. See how our expertise and Advanced Identity Authentication can help add security, convenience, privacy, and productivity to the enterprise operation you wish to improve.

iCAM7 series

iCAM7000 | iCAM7010-U1 | iCAM7101 | iCAM7111-U1T (Titanium Color)

iCAM TD100

Best Biometric Solution / award

Iris ID Systems, Inc.

7 Clarke Drive
Cranbury, NJ 08512
Tel: +1-609-819-IRIS(4747) Fax: +1-609-819-4736
Email: sales@irisid.com
www.irisid.com

IrisAccess®

formerly LG IRIS

As BiometricUpdate.com reported in October 2014, the Indian government plans to use its national Aadhaar biometric database to deploy its newly-proposed universal healthcare program. As part of the new national government's manifesto, Prime Minister Narendra Modi has promised radical reforms in healthcare with the introduction of the "National Health Assurance Mission" (NHAM) scheme. The new program's goal is to provide accessible and affordable healthcare to every Indian citizen.

In order to achieve this goal, the Indian government intends to use Aadhaar as a means of identification for healthcare insurance beneficiaries. The new government decided to extend the use of the system to other social programs and to make Aadhaar the primary national identity scheme after extensive review. A government source told the Economics Times newspaper that: "The government has planned to seed Aadhaar numbers with its universal health program. Experts think that this would help in keeping a check on any fraudulent insurance claims or ghost beneficiaries."

Aadhaar, the world's largest biometric database, is governed by the Unique Identification Authority of India (UIDAI), and is currently used to authenticate delivery of social services including school attendance, natural gas subsidies to India's rural poor, and direct wage payments to bank accounts.

The introduction of universal healthcare to India's citizens will arguably be the most ambitious use of the biometric database. To date, India only spends 1.04 percent of GDP on publicly funded health, which is one of the lowest amounts in the world. Higher amounts of public health finance are pivotal to provide a wider range of essential basic health services, along with access to life-saving drugs and expanded health care facilities, such as hospitals and health centers. Because the government plans to make the healthcare plan accessible through Aadhaar, it has committed to accelerate resident registration. In its first budget, the government allocated $340 million to speed the Aadhaar registration process. The Indian government's objective is now to enroll 100 million more residents with Aadhaar. UIDAI has already enrolled about 700 million people and issued unique identification numbers to 650 million.

In Ghana, a National Health Insurance Scheme (NHIS) was introduced in 2003 to improve access to basic health care for all Ghanaians, with a special emphasis on the underprivileged. By 2013, the National Health Insurance Authority (NHIA) had 10 million active subscribers representing 38 percent of the population. Remarkably, there were 26 million names in its central database – 2 million more than the national population and a strong indication that there was a problem with multiple registrations. Other challenges that plagued the scheme included an increase in the number of claims and the average claimed amount as well as ID card management issues. To clean up its membership database and to deal with card management challenges and claim fraud, the NHIA engaged GenKey through its partner, STL Technologies, to introduce biometric membership registration, database deduplication, instant issuance of ID cards and biometric verification at the healthcare provider.

GenKey is a leading provider of large-scale biometric identity management solutions for digital health care, with a focus on emerging economies. Building on its unique strength of high-speed deduplication, GenKey has developed complete solutions for both medical identification handling and claim processing, along with large-scale ID management. More than 50 million people use GenKey's high-quality solutions.

The biometric registration process begins with subscribers visiting a NHIA Scheme (Registration) Office and providing their biographic information and fingerprint samples. Before member data

is permanently added to the member database, GenKey's Automated Biometric Identification System (ABIS) compares the fingerprint samples with all persons already in the database. Any duplicates detected by the ABIS are manually adjudicated by an adjudication officer who, supported by a dedicated software application, inspects all potential duplicates and decides which of them to accept as genuine. Once this process is completed, the system retrieves the relevant biometric and biographic information from the central database and instantly personalizes and prints a smart card for the member. The entire process of capturing a member's data, deduplication, card personalization and printing is typically completed within 7 minutes.

To curb the rising cost of claims and medical claim fraud, the NHIA is also introducing biometric verification at the health care provider. When a card holding member visits a health care provider, their fingerprint data is captured and matched against the fingerprint template stored on their member card during registration. If verification is successful, an irreversible claim verification code (CVC) is generated and entered on the member's claim form. The CVC is based on biographic data, context information (such as health care provider ID, service date and membership ID) and the result of the biometric verification. Because the CVC can only be generated correctly if the member is present at the time the claim is generated, it acts as a biometric proof-of-presence, thus eliminating fake and duplicate claims from healthcare providers.
A nation-wide rollout of the biometric membership registration and instant issuance of the ID card system started in January 2014 and is currently running in four regions of Ghana. So far, over 4 million subscribers have been successfully registered using the new system. The initiative to adopt biometric technology in the healthcare system is expected to lead to a duplicate-free member database, protection of data integrity and improved efficiency in service delivery.

Instant issuance of member ID cards at the point of registration has also eliminated delays in ID card production. These benefits, together with the drastic reduction in fraudulent claims through biometric authentication at the point of service delivery offer long-term benefits to Ghana's health care.

In terms of adoption, the appeal of biometric health care for patient identification solutions obviously lies with its inherent benefits. Patient identification solutions offer the option to identify proper insurance status, thereby increasing fraud protection. Another key benefit is safety. With the use biometrics, a verified patient obtains the correct treatment. Further, the use of biometrics is quick and efficient, eliminating the need for keying in data which can lead to unreliable data. These systems are also beneficial since they work for unresponsive patients. The driving objective behind biometric health care is therefore to combine high security with convenience.

As organizations adopt technological roadmaps that embrace higher security through biometrics, the next hurdle will be implementing patient identification solutions and creating open networks for patients to access their medical records across a multitude of providers and platforms.

With imminent changes to the U.S. health system and as medical record management capabilities change with technology, patient identification mechanisms will undoubtedly follow suit. The capabilities and scalability of biometrics with regard to patient identification removes many risks of forgery, misidentification and record security.

BIO-key, as an example, has been building the foundation for patient ID through the firm's longstanding relationship with blood centers in the United States. To date, the company has issued more than three million donor identification licenses, which is more than any other biometric

GenKey ClaimSync

Medical Claim Management Solution

GenKey ClaimSync is a biometric-based solution for handling and simplifying medical claims while minimizing related claim fraud. The solution brings these benefits for both public and private health initiatives, healthcare providers and insurance companies.

claimsync

Preventing medical fraud and identity theft while improving patient safety

Fraudulent claims and identity theft are important concerns in healthcare and medical claim systems. Medical fraud may result in losses of hundreds of millions of dollars every year. Medical identity theft is a concern for both healthcare providers and patients. Incorrect identification can put a patient's health at risk and may even lead to life-threatening situations.

Medical identity theft is the fastest growing form of identity theft and jeopardizes safety

GenKey ClaimSync is a cost-effective solution to:

- secure patient privacy and safety
- reduce fraud in the handling of medical claims
- improve data integrity of the entire process
- simplify the vetting process and automate the claim process

The solution is based on **GenKey's Automated Biometric Identification Solution (ABIS)** and **BioHASH® verification**, providing:

- biometric member registration
- large-scale biometric-based deduplication
- biometric member (patient) verification
- biometric check on the medical claim

Why use GenKey ClaimSync?

- Simple but robust member verification
- Tamper-resistant claim generation/verification using unique biometric proof-of-presence
- Simple, efficient and transparent claim vetting
- Easy integration into existing systems of member registration and claim handling

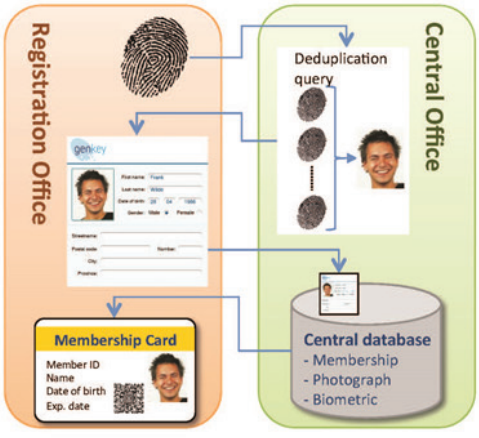
GenKey's biometric technology ensures accurate patient identification and patient privacy. BioHASH® protects biometric information using an irreversible cryptographic hash function.

Biometric Registration

Obtaining a duplicate-free member database

The first step involves biometric enrollment of the members. This takes place at the **Registration Office**, when people register for the first time or renew their membership of a healthcare scheme.

Registration of a **new member** consists of the electronic collection of the biographical data and biometric data, such as the facial picture and the fingerprints of the applicant. The fingerprint information is sent to the **Central Office**, where a biometric duplicate check is performed. If no duplicate is found, a member ID number is issued and a



www.genkey.com

genkey

membership card is generated on which the picture, name, ID number, expiration date, etc. are printed. The privacy protected biometric information as well as the expiration date is also added to the card in the form of a 2-D barcode or written to a chip in the card.

- In the case of an **existing member**, the member's data are retrieved from the Central Office and verified manually. Fingerprints of the member are taken and sent to the Central Office for a duplicate check. If no duplicate is found, a new membership card, containing the membership data and the privacy protected biometric data, is issued.

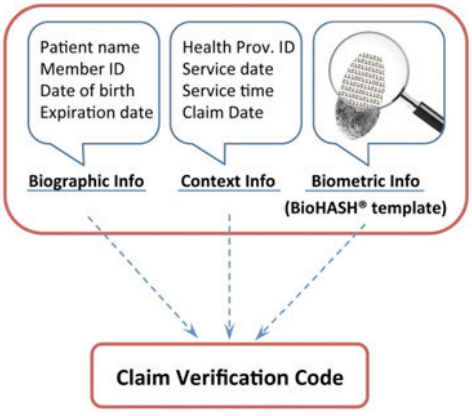
Member (Patient) Verification and Claim Generation

Ensuring the right person gets the right service

- During a visit of a member (patient) to a Healthcare Provider (e.g., a hospital or a local clinic), information is read from the barcode or chip on the membership card and verified. The fingerprint information stored on the card is compared with a live measurement of the fingerprint.

Accurate patient identification prevents medical errors and enhances patient safety

- In case of a successful member verification, the system generates a **Claim Verification Code**, based on:
  - Biographic data (patient name, member ID number, etc.)
  - Context information (Healthcare Provider ID number, service date and time, claim date, etc.)
  - Biometric data (fingerprint information) based on privacy respecting BioHASH® technology.



Tamper-resistant electronic claim generation

- The Claim Verification Code acts as a **proof-of-presence**: it ensures that *the* member was present at *the* Healthcare Provider at *the* time that the claim was generated. The Claim Verification Code is added to the claim form as a unique biometric signature.

Because the Claim Verification Code can only be generated if the member is present, possible fraud such as issuing fake claims is prevented

- After medical treatment, the medical professional completes the claim by filling in treatment details and the claimed amount. This information is sent to the Claim Processing Center.
- On-line but especially also off-line processes are supported. The Claim Verification Code is composed of a few-digit number, which can be manually written on the claim.

Claim Vetting and Tracking

Simple and traceable vetting of claims

- At the Claim Processing Center, the information in the claim is verified using claim vetting software. Relevant claim data (biographic data, context information and the Claim Verification Code) are sent to the Central Office. Based on the data in the central database, the Claim Verification Code (proof-of-presence) is checked.

The result of the check is sent back to the Claim Processing Center, where appropriate actions can be taken in the vetting process.

Transparent claim tracking

- The offered solution ensures a transparent claim tracking process by verifying membership at the Healthcare Provider and verifying the validity of a claim based on a biometric proof-of-presence. Moreover, the solution can easily be incorporated in existing medical claim systems.

High Tech Campus 9, 5656 AE Eindhoven, the Netherlands, info@genkey.com
www.genkey.com

genkey

company. GenKey also provides a powerful integrated medical claim management solution, which is outlined below.

4. Medical Biometrics

In contrast to health biometrics, personal medical data, which includes digital images and biorhythm recordings, are referred to as "medical biometrics." Such data is produced in ever-increasing quantities and is used for diagnostic and therapy purposes. Medical biometric research aims to use personal medical data sets, such as images and biologically-measurable signals, for solving medical problems and to provide high-performance services in the medical field.

Medical biometric systems integrate multiple technologies from the fields of biology, medicine, consumer electronics, statistics and ubiquitous computing to create systems of computer-aided diagnosis and therapy. Previously such systems were expensive and contained to medical facilities, but increasingly, such systems are becoming miniaturized and integrated into wearable technologies, such as bracelets, headbands and watches. These devices will be able to provide medical diagnostic data through Internet-based cloud applications in the near-term.

In a previous Biometrics Research Group research note, we determined that the next generation of consumer electronics will focus on measuring biorhythms.

Biorhythms are defined simply as the rhythms of life, and include vital body functions, including heart rate and blood pressure. Medical chronobiologists have found that biologic rhythms can affect the severity of disease symptoms, diagnostic test results, and even the body's response to drug therapy.

Now these investigators are working to measure how the rhythms of life can be monitored through microtechnology to improve the practice of medicine and health. The result is the emergence of wearable and even ingestible sensors developed by firms such as Proteus Digital and BodyMedia.

Biometrics Research Group, Inc. estimates that wearable health and fitness sensors will exceed 40 million shipments by 2015. Currently, the research firm projects that well-known sportswear firms such as Adidas and Nike will drive early adoption, companies such as Proteus Digital and BodyMedia will drive cutting edge technological developments, and devices will be mainstream by the end of the decade.

Nike is well-known for its Nike+iPod sports kit, which measures and records the distance and pace of a walk or run through embedded shoe sensors that connect to an iPod. Adidas has a similar system entitled miCoach, which tracks running space, distance, time and calories through GPS-enabled mobile phone devices.

As reported previously in BiometricUpdate.com, a wide range of other biometric fitness and healthcare applications have entered the market, including wireless and wearable activity and sleep trackers and even smartphone-enabled cardiograms.

The next stage in the technical revolution will be biochemical sensors that monitor and record biorhythms from within the body. Proteus Digital has developed wearable and ingestible sensors that work together to detect ingestions and physiologic data.

By capturing objective information and providing actionable insights, patients using the technology can take control, communicate with caregivers and clinicians, and improve their health. The company has developed an ingestible sensor, which is completely made of ingredients found in food, and that is activated when swallowed.

The sensor is taken alongside medications, and is powered by the body's biochemistry. The body therefore actually powers the sensor. With no battery or antenna, stomach fluids completely power the device and organically transmits the data generated by sensor.

A patch, body-worn and disposable, captures and relays the body's physiologic responses and behaviors. The patch receives the data from the ingestible sensor, detects heart rate, activity and rest and forwards that information to a Bluetooth enabled mobile device. The device, which can be carried in a purse or pocket, provides secure access to metrics that can be used by consumers, caregivers, clinicians, caseworkers, drug and device makers and health management systems.

The company caters to consumers to help them better manage their health and improve how they communicate with their care network. Family caregivers can use the technology to stay connected and monitor the health of their loved ones. A great beneficiary of the technology are clinicians who can make better decisions about their patients through more accurate monitoring between doctor visits. In terms of corporate and organizational users, caseworkers in the social welfare, corrections and healthcare sector can leverage Proteus Digital's "digital health feedback system." Caseworkers can manage multiple clients at once, monitoring mandated or illicit drug use. Health systems can use the technology to understand demographic patterns and determine how to improve overall health care. Drugs and device makers are also able to utilize Proteus Digital's technology to improve health outcomes by measuring pharmaceutical and device effectiveness.

In terms of newer wearable technologies, body monitoring pioneer BodyMedia unveiled a newer generation of its BodyMedia CORE device, the activity and health armband used on the Biggest Loser television show.

Incorporating four sensors into a housing smaller than an iPod Nano, the CORE 2 is the world's smallest wearable multi-sensor device, as well as the first to offer a choice of interchangeable jewelry and other accessories, including faceplates, straps and even cufflinks.

The device also features a new heart rate monitoring option; Bluetooth technology enabling live activity updates on a smartphone or tablet, as well as longer battery life; and data-rich mobile and online apps that can help users make smart food, exercise and lifestyle-related health decisions daily.

With a literal explosion of new biorhythm monitoring technologies, Biometrics Research Group, Inc. expects the biorhythm monitoring market to reach $100 million in sales by 2015, thereby enhancing the bottom line for consumer electronics retailers. Indeed, wearable computing was a key highlight at the at the 2015 Consumer Electronics Show.

The Consumer Electronics Association, which organizes the annual trade show, projects that U.S. wearable unit sales will reach 30.9 million units, up 61 percent, and generate US$5.1 billion in revenue in 2015. This represents a 133 percent increase in revenue streams.

According to CEA, most of these wearables will be fitness bands and trackers, along with smart watches and eyewear. A wide number of products based on biorhythms were demonstrated at the show.

For example, Garmin announced and demonstrated new additions to its wearable product selection, including its new Vivoactive smartwatch. Building upon Garmin's Vivofit sports band, the new smartwatch offers consumers lifestyle tracking functions, as well as built-in GPS functionality and smartphone notifications.

Another impressive device that debuted was the second iteration of heart rate monitors from Mio Global. The award-winning company claims to be the first to have introduced a wrist-based monitor that does not require sensors strapped to the chest.

The company's Mio Alpha 2 device features a heart rate monitor that connects via Bluetooth to Android mobiles and iPhones to feed heart rate data directly into the app that consumers have installed onto their

phones. The company also demonstrated its Mio Fuse sport activity tracking wristband, which provides EKG-quality heart rate monitoring.

Another company making headway into the biorhythmic wearable space is Valencell. Before the show, the firm announced that it had licensed its PerformTek biometric technology to a number of technology companies including Intel, Jabra, Atlas, and Scosche, many of which showcased its underlying technology at CES.

Products include Jabra's Sport Pulse Wireless Earbuds, Scosche's Rhythm+ and Rhythm Smart Heart Rate Arm Band Monitors, SMS Audio's BioSport In-Ear Wired Ear Bud, iriver's iriverON Heart Rate Monitoring Bluetooth Headset, LG's Heart Rate Earphones, and ATLAS Wristband.

In addition to current products on the market, Valencell also announced that it has begun partnering with first responder and gaming industries to integrate biometric technology into various applications to provide an improved and highly-connected experience.

The explosion of biorhythmic technology was highly apparent at CES. Industry analysts from CEA and other market research firms expect the fast pace of innovation and product releases to continue unabated into 2015.

5. Securing Mobile Healthcare Applications

Mobile health, also known as mHealth, is a term used for the practice of medicine and public health supported by mobile devices. The term is most commonly used in reference to using mobile communication devices, such as mobile phones, tablet computers and personal digital assistants (PDAs), for health services and information.

mHealth is a subset of eHealth, which is the use of information and communication technology (ICT), such as computers, mobile phones, communications satellite, and patient monitors for health services and information. mHealth applications include the use of mobile devices in collecting community and clinical health data; delivery of health care information to practitioners, researchers, and patients; real-time monitoring of patient vital signs; and direct provision of care via mobile telemedicine.

mHealth is an increasingly popular consideration because of its capacity to increase access to health care and health-related information, particularly in hard-to-reach populations and in developing countries. mHealth applications can improve the ability to diagnose and track diseases and can provide timelier, more actionable public health information. Further, mHealth applications can provide expanded access to ongoing medical education and training for health workers.

Due to the sensitivity of the data being collected and relayed vis-a-vis mHealth applications, Biometrics Research Group, Inc. expects that biometric technology will be highly leveraged to protect mobile health devices, applications and resources in the future. We anticipate that fingerprint recognition technology will be utilized the most since it is the primary biometric technology utilized in smartphones and other mobile devices. Indeed, fingerprint technology is in the limelight thanks to Apple, Samsung and other device manufacturers, who have removed the mystique around biometrics by introducing the technology to the consumer. Fingerprint recognition is therefore becoming a globally accepted method for positive identification and we expect it to be increasingly used in mHealth applications.

Summary

Since inefficiency and fraud are overriding administrative concerns for health care systems, especially in the United States, we can expect increased investment in health care security protocols that involve biometrics. Adoption of

"health care biometrics" will mainly take place in hospitals, clinics and other facilities. In terms of workflow, these tools will protect health care resources and medical data. Concerning patients, biometric systems will be used for patient identification. While small-scale implementations will be used in the United States, we expect that large-scale patient identification systems will be rolled out in emerging and developing countries. Medical biometrics will continue to develop into a growth market due to the increasing demand for "wearable" consumer electronics. The increasing use of mHealth applications will also drive the utilization of biometric authentication for security purposes.

About the Biometrics Research Group, Inc.

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.

Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.

INTERPOL WORLD 2015

14 - 16 APRIL 2015

Sands Expo & Convention Centre, Singapore

PLAN YOUR VISIT NOW

CYBERSECURITY

BORDER MANAGEMENT

SAFE CITIES

SUPPLY CHAIN SECURITY

YOUR PARTNERSHIP PLATFORM

INTERPOL *World* Public-Private Partnership

- Game-Changing catalyst of innovation to address global security challenges

YOUR SOURCING & BUSINESS PLATFORM

INTERPOL *World* Expo

- 250 exhibitors from over 25 countries
- Be the first to view new and innovative technologies

YOUR KNOWLEDGE & NETWORKING PLATFORM

INTERPOL *World* Congress

- Launchpad of co-created innovative solutions with leading private-sector security solutions providers

EARLY BIRD ENDS 27 FEB 2015

(LIMITED SEATS ONLY!)

YOUR BUSINESS AND NETWORKING ENGINE

Register online now at www.interpol-world.com

Event Owner

INTERPOL

Supported By

MINISTRY OF HOME AFFAIRS

SINGAPORE EXHIBITION & CONVENTION BUREAU

Supporting Knowledge Partner

FROST & SULLIVAN

Held In

YourSingapore

Managed By

mp