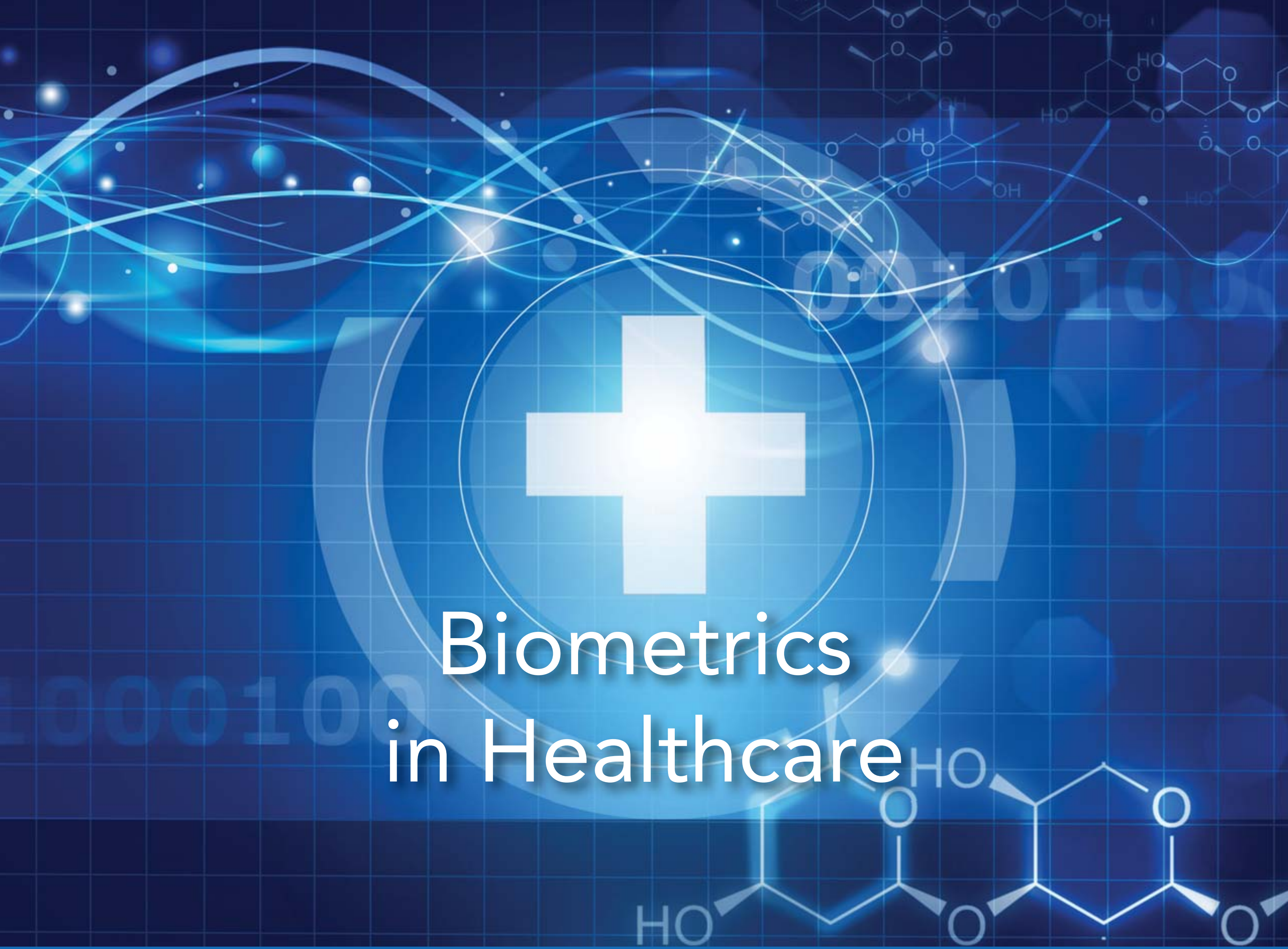


Biometrics in Healthcare

BIOMETRIC
UPDATE.COM

Biometrics will continue to drive technological transformation within the global healthcare market to provide meaningful cost savings through fraud reduction and increased workplace efficiency, while simultaneously improving and expanding care delivery to patients over the long term. Biometrics Research Group, Inc. expects that the entire global marketplace for biometric solutions in the healthcare market will reach approximately US$5 billion by 2020.

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

Chris Burt, Contributing Editor, BiometricUpdate.com

All content, including forecasts, analysis and opinion, has been based on information and sources believed to be accurate and reliable at the time of publishing. Biometrics Research Group, Inc. makes no representation of/or warranty of any kind as to the accuracy or completeness of any information provided, and accepts no liability whatsoever for any loss or damage resulting from opinion, errors, inaccuracies or omissions affecting any part of the content.

About the Biometrics Research Group

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 startups 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 in 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.

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.

HID®

NURSES
DOCTORS
ADMINISTRATORS
PATIENTS
VISITORS
CONTRACTORS
STAFF
IDENTITIES SECURED.

When identity security is as important as work-flow efficiency, hospitals turn to HID Global for the most advanced multi-factor authentication solutions in the world. Through a single credential, you can effectively manage both your facility and network access simply, conveniently and compliantly. Our secure identity and access management solutions are transforming the ways hospitals identity proof, authenticate, grant and revoke access to electronic medical records, narcotic prescribing, and claims data. Find out how to increase identity security and workflow efficiency while minimizing risk and liabilities by visiting hidglobal.com/healthcare.

You'll call it healthcare authentication solutions you can trust. We call it, *your security connected.*

YOUR SECURITY. **CONNECTED** | hidglobal.com/healthcare

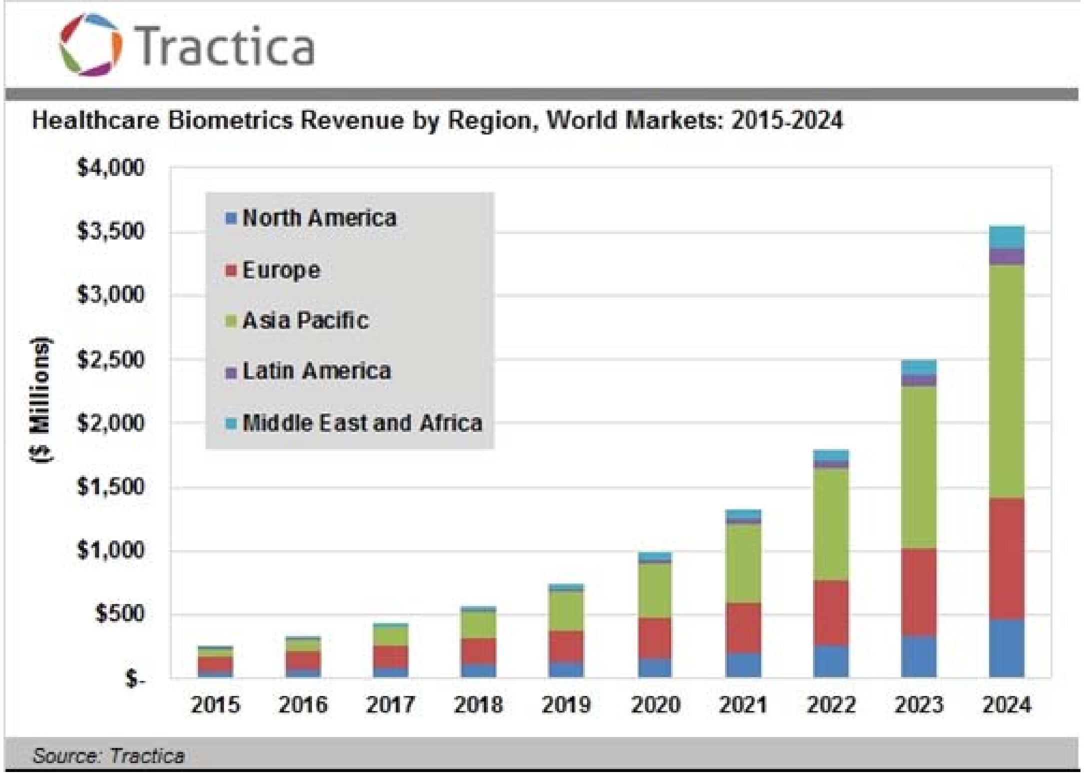
Executive overview

Biometrics will continue to drive technological transformation within the global healthcare market to provide meaningful cost savings through fraud reduction and increased workplace efficiency, while simultaneously improving and expanding care delivery to patients over the long term.

Market Overview

Biometrics Research Group, Inc. estimated in 2015 that the entire global marketplace for biometric solutions in the healthcare market will reach approximately US$5 billion by 2020. Biometric use will reflect the increasing demand for healthcare fraud prevention and cost containment in the United States, along with the need to improve patient privacy and healthcare safety. Solutions that can meet both regulatory and usability demands will drive increased adoption for both government-delivered and private healthcare services in the U.S. and throughout the world.

In 2015, market analysis firm Tractica projected that the global healthcare biometrics market will grow from its base of US$250 million in 2015 to reach US$3.5 billion by 2024. Tractica anticipates that the key healthcare use cases will include home and remote patient access, care provider authentication, patient identification and tracking, and pharmacy dispensing. These use cases will be caregiver-facing except the latter, which will be consumer-facing. The consumer use of accessing personal medical information from home or remote locations is likely to be a low-price but high-volume software solution, and is forecast by Tractica to generate approximately 60 percent of all revenue. In comparison, the other three caregiver-facing use cases will be mostly hardware-driven and represent high unit prices but lower volumes.



Healthcare Biometrics Revenue by Region, World Markets: 2015-2024

Source: Tractica

In 2015, research consultancy Transparency Market Research forecast that the global healthcare biometrics market will grow to US$5.8 billion in 2019, from approximately US$1.2 billion in 2012, representing a compound annual growth rate (CAGR) of 25.9 percent from 2013 to 2019. The firm notes that the use of biometrics in the healthcare industry not only ensures minimization and prevention of fraud, data loss, and resource wastage, but also enhances the quality, privacy, and safety of hospitals. They note that the cost of biometric systems is not very high and these systems function with utmost accuracy and performance, thereby making it a wise and cost-effective investment for healthcare security applications. Additionally, Transparency Market Research groups the healthcare biometrics market into major applications of physical access control, logical access control, and transaction authentication, while segmenting regions into North America, Europe, Asia-Pacific, and rest of the world. North America and Europe collectively make up 75 percent of the global market share, according to the research firm.

Healthcare Biometrics

Biometrics in the healthcare industry are primarily used for staff authentication and patient identification solutions. Biometrics Research Group defines "healthcare biometrics" as biometric applications in doctors' offices, hospitals, or for use in monitoring patients. This can include access control, identification, workforce management or patient record storage. Many hospitals and healthcare organizations are currently deploying biometric security architecture. Secure identification is critical in the healthcare system, not only to control logical access to centralized archives of digitized patients' data, and to limit physical access to buildings and hospital wards, but also to authenticate medical and social support personnel.

The need to identify patients with a high degree of certainty is also an increasing challenge for healthcare organizations. Identity verification solutions based on biometric technology can provide identity assurance and authentication while increasing privacy and security. Biometric technology can add operational efficiencies to the healthcare system that reduce costs and fraud, and increase patient satisfaction by reducing medical errors.

Healthcare and Fraud

As Goode Intelligence notes, there have been a significant number of high-profile incidents in the healthcare industry in which criminals have targeted large depositories of medical identity information. In fact, per the Identity Theft Resource Center, the healthcare sector accounted for 42.5 percent of total cases of identity theft, the highest rate of any industry.

While there are no exact figures on the cost of healthcare fraud in the U.S., annual losses are estimated in the billions of dollars. The Federal Bureau of Investigation (FBI) estimates that between US$75 and US$250 billion is lost annually in healthcare programs nationwide, based on the assumption that fraudulent billings to public and private healthcare programs make up three to 10 percent of total healthcare expenditures.

Other estimates have placed total annual losses to healthcare fraud at between US$125 and US$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 Healthcare Anti-Fraud Association, an organization of consisting of approximately 100 private insurers and public agencies, US$69 billion is lost annually in all healthcare programs nationwide, based on 2010 calculations of three percent of national health care spending.

Goode Intelligence has noted that 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 cost data for private insurance fraud is not publicly available, many examples of private insurance security breaches abound. In 2015, health insurer Excellus BlueCross BlueShield announced that it was hacked in 2013, with data from more than 10 million of its customers stolen. This followed news from the second largest health insurer in the U.S., Anthem, which had also suffered a major data breach in 2015 causing 78 million accounts to be exposed.

Concerning government fraud, during the 2011 fiscal year, the U.S. Department of Justice, 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 healthcare programs, which represents the highest amount ever recovered in a single year. However, this record-breaking recovery accounted for 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 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 healthcare 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 that 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 prescriptions or selling prescription drugs, using transportation benefits for non-medical related purposes, and loaning or using another's insurance card.

Typically, when healthcare fraud is perpetrated, the provider passes the costs along to its customers. Due to the pervasiveness of healthcare fraud, approximately 10 cents from every dollar spent on healthcare in the U.S. goes toward paying for fraudulent healthcare claims.

Federal law 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 healthcare provider that ends in a conviction can have serious consequences. The healthcare 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 healthcare 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, palm prints, and iris scans to gait, facial, or even voice recognition. Biometrics-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.

As electronic health records (EHRs) and personal health records (PHRs) become more commonly used, biometrics will be utilized as an authentication mechanism by both medical facilities and insurers. In some developed countries, including the U.S., 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. Several biometric equipment manufacturers and service providers offer turnkey applications that maintain and track access to EHRs.

Goode Intelligence notes that the Health Insurance Portability and Accountability Act (HIPAA), as enacted in 1996, covers the regulation of the U.S. healthcare industry. Biometric verification of identity is a regulatory component of "Technical Security Services to Guard Data Integrity, Confidentiality, and Availability", and is included as a "unique user identification method. Biometrics is therefore seen as one of the important tools to ensure compliance with HIPAA, especially the privacy rule and its application to Protected Health Information (PHI).

Because inefficiency and fraud are overriding administrative concerns for the healthcare system within the U.S., Americans can expect increased investment in healthcare security protocols that involve biometrics. Adoption of "healthcare biometrics" will mainly take place in hospitals, clinics and other facilities. Biometrics in healthcare often takes two forms: providing access control to resources and patient identification solutions.

In terms of workflow, such access control tools protect healthcare resources and medical data. Concerning patients, biometric systems are used for patient identification. While small-scale implementations will be used in the U.S., we expect that large-scale patient identification systems will be rolled out in emerging and developing countries.

Healthcare Growth & Technological Innovation

In 2014, the Indian government announced that it planned to use its national Aadhaar biometric database to deploy its newly proposed universal healthcare program. Aadhaar is the 12-digit unique identification number issued by the Indian government to every individual resident of India. The Aadhaar project aims to provide a single, unique identifier which captures all the demographic and biometric details of every Indian resident. Currently, the government has issued over 900 million Aadhaar numbers and over one billion people have now been enrolled in the scheme.

As part of the national government's agenda, 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 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 healthcare facilities, such as hospitals and health centers.

In the U.S., in contrast, healthcare is one of the most important expenditure categories within the national economy. According to the World Health Organization (WHO), total healthcare 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 the end of this year.

In 2013, U.S. healthcare spending reached US$2.9 trillion, or US$9,255 per person, and generated billions of claims from millions of healthcare 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 healthcare 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 healthcare in the U.S., it is estimated that 31 percent is allocated to hospital care, 21 percent to physician and clinical services, 10 percent to medication, four percent to dental, six percent to nursing homes and three percent to home healthcare. 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. Healthcare expenditures are predicted to reach US$4 trillion by the end of this year.

Despite high levels of spending on healthcare, relative to other industrialized countries, most analysts rank the U.S. last in the quality of care provided, based on economic investment versus actual health outcomes.

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

Consequently, there are wide gaps in insurance coverage, along with a wide number of healthcare services providers. Over the past decade, political efforts to reform healthcare provision have led to deep partisan division. The Obama administration sought to make coverage more accessible and affordable through the private market to a wider number of uninsured people through the Patient Protection and Affordable Care Act.

The Affordable Care Act was designed to increase health insurance quality and affordability, lower the uninsured rate by expanding insurance coverage and reduce the costs of healthcare. It introduced mechanisms including mandates, subsidies and insurance exchanges. The law requires insurers to accept all applicants, cover a specific list of conditions and charge the same rates regardless of pre-existing conditions or sex.

The ACA caused a significant reduction in the number and percentage of people without health insurance, with estimates ranging from 20-24 million additional persons covered during 2016. Further, increases in overall healthcare spending have slowed since the law was implemented, including premiums for employer-based insurance plans. The Congressional Budget Office reported in several studies that the ACA would reduce the budget deficit, and that repealing it would increase the deficit.

Republicans have opposed the Act due to the increased tax burden it has created on higher income earners, along with higher premiums and deductibles levied through exchanges, along with the perceived lack of choice due to imposed mandates upon individuals. With the alignment of the Trump administration and the Republican-controlled Congress, there will be pressure to introduce effective healthcare legislation that will address these criticisms. While ideological division will ensure that universal health coverage is not adopted in the U.S., cost containment will continue to be an important consideration, and a primary driver for the use of biometrics, regardless of what reforms are implemented.

Due to this fact, the U.S. will dominate the market for biometric healthcare offerings, and will benefit from the development of biometric platforms that support multi-modal biometric identity, along with the growing availability of biometric solutions to combat fraud and improve patient privacy and safety. Biometrics will also be increasingly used for medical monitoring and mobile healthcare.

Biometrics and Healthcare Cost Containment

One of the most significant challenges facing healthcare today is the need to reduce costs while improving the quality of care. At the center of this challenge is the ability to efficiently ensure the proper identification of both healthcare professionals and their patients. Not only are there significant risks associated with the improper identification of staff or patients but all of the healthcare constituencies (providers, payersand patients) suffer greatly when inefficient and inadequate identity and access control mechanisms are employed.

Moreover, the failure to correctly identify patients invites fraud and creates another serious problem: patient ID theft. Unlike banking fraud where the risks are mostly financial, patient ID theft can not only lead to costly medical errors, but also limit access to critical services by those who need them most, dramatically increase costs and even result in serious injury or loss of life.

Whether considering developing markets where government-sponsored healthcare is a critical service being offered to citizens, or developed markets where both government and commercial stakeholders struggle to balance costs and care, the central problem is how to ensure that the right people are getting the right services at the lowest possible cost.

These challenges place a significant burden on currently deployed identity management technologies. Unfortunately, many of these systems are difficult to deploy, hard to use and inefficient. What is needed to solve this identity management problem is a solution that is both secure and convenient for all constituents.

Rather than placing barriers in the path of patients and healthcare workers in the name of security, providers can choose secure identity solutions that are robust, reliable, efficient and convenient. This is where biometrics can make a significant difference. For several years now biometrics have been deployed in a variety of healthcare use cases ranging from medical dispensing and the electronic prescription of controlled substances (EPCS) to real-time patient identification for medical services.

Patient registration at check-in

A fingerprint authentication solution is used today for patient registration by a world-renowned healthcare provider in the U.S.. A leader in innovation, this large integrated health system constantly assesses new tools and methods to deliver accurate, cost-effective care. As the obvious solution to the problem of patient misidentification, biometric authentication was implemented at patient registration locations to help reduce medical errors, increase productivity — and improve patient satisfaction.

In traditional patient registration, the patient provides proof of identity and insurance with a variety of cards and documents. This time-consuming system was replaced at hundreds of points of registration by an advanced biometric authentication system that streamlines the patient check-in process. To register, a patient simply provides their name and date of birth, and places their pre-enrolled finger on the fingerprint sensor to verify their identity. In this way, the biometric authentication solution helps to ensure that the patient is linked to their own medical record so accurate insurance information can be confirmed, and the appropriate care can be provided. In some instances, co-pays can be paid and applied using the same system.

This authentication solution, provided by Certify, uses HID Global Lumidigm fingerprint sensors because of the superior performance characteristics of multispectral imaging technology. A successful authentication solution must incorporate a sensor that provides intuitive, single-try capture for all patients, regardless of their age or health, while simultaneously performing liveness detection to ensure that the fingerprint being presented is not a fake. The sensor technology must also perform highly accurate matching. The Lumidigm technology was selected by this respected healthcare provider because it excels at these performance requirements. The biometric data is managed by the Certify cloud-based service and is kept separate from protected patient information, further protecting patient privacy.

Biometric patient registration at this large provider decreased the number of staff required to check patients in and out, reduced medical errors resulting from improper patient identification, and decreased the number of insurance claims denied as a result of human error or incomplete registration information. Certify notes that this biometric authentication solution reduced patent check-in time by an average of 12 minutes, increasing staffing efficiency and enhancing the patient experience. With biometric authentication, patients spend less time at check in, are not required to produce ID and insurance documentation, and have fewer errors in their records or billing. They can be confident that the provider is delivering appropriate care based upon who they are.

Government health benefits

Similar benefits were realized by a Latin America country's large public health system when it implemented Lumidigm biometrics from HID. In addition to the challenges faced by the large U.S. provider discussed above, this government healthcare system was serving patients throughout the country, including at mobile rural clinics. Reducing fraudulent access to healthcare was the main driver of biometric adoption, and reliable fingerprint image capture was critical to the success of the authentication program. The Lumidigm technology successfully operated in real world situations such as for patients with rough and dry skin and in diverse outdoor climates — usage conditions beyond the capabilities of conventional fingerprint sensors. More than 28 million users have benefited from biometric authentication in this program, allowing vulnerable populations in the country to access basic health service. The provider reports that the biometric authentication solution facilitates faster access to medical services by authorized patients, while reducing fraud and government cost.

A recent report from the Ponemon Institute states that the primary root cause of patient misidentification is incorrect identification of patients at registration, and that the use of biometrics can reduce patient misidentification. The two examples above bear this claim out: where biometrics have been deployed, there have been significant improvements to costs and patient safety, along with enhanced patient convenience. Ponemon goes on to say that biometric registration could reduce denied insurance claims by 25 percent. Significant improvements have also been realized in control and access to medical dispensing systems, virtually eliminating theft of controlled substances. Mandates by the US Drug Enforcement Agency (DEA) for electronic prescriptions of controlled substances (EPCS) impose compliance requirements which can be met with significant cost and time savings by utilizing these systems.

Biometrics Research Group, Inc. projects that the following companies will dominate the biometric healthcare sector:

HID Global

HID Global provides innovative products, services, solutions, and know-how related to the creation, management, and use of secure identities in the financial, education, enterprise, government, and healthcare industries. The company's served markets include physical and logical access control, with strong authentication and credential management; card printing and personalization; visitor management systems; highly secure government and citizen ID; and identification RFID technologies used in animal ID, industry and logistics applications. The company's primary brands include ActivID®, EasyLobby®, FARGO®, IdenTrust®, LaserCard®, Lumidigm®, Quantum Secure, and HID®.

The company has recently updated several products for the healthcare market. It launched its HID PIV (Personal Identity Verification) solution, an end-to-end system for managing access to doors, IT systems, networks, and data for high-security and regulated industries, including healthcare. Its biometrics line of Lumidigm fingerprint sensors has been enhanced with the addition of liveness detection and better usability for its M-Series fingerprint products.

Lumidigm multispectral fingerprint imaging technology is field-proven in many applications, including validating over 28 million patient IDs for a Latin American government healthcare program; securing over 1 million dispensing transactions of medical items per week by hospital nurses; authenticating over 85 million bank customers making more than 4 billion ATM transactions per year; and verifying the identity of over 300,000 citizens per day at a major land border crossing.

As the industry shifts its focus to ID technology, institutions are slowly changing the way they operate, how they manage access to patients, data and equipment, how they protect patient privacy, and how they improve billing accuracy, while still providing the same level of healthcare, according to HID Global.

"Healthcare organizations are increasingly seeking to improve the physician, staff and patient experience by employing a combination of strong authentication and new IoT applications to address their challenges," said Sheila Loy, director of healthcare industry with HID Global.

"Trusted identities will simplify and connect all aspects of healthcare operations, from opening hospital doors, accessing healthcare records and e-prescribing of controlled substances, to how healthcare professionals interact with patients and log their activities."

HID Global has identified three key technology trends that the healthcare industry is adopting to establish, create, manage and use trusted identities.

The first trend is a move towards deploying integrated, compliant systems that are both convenient and connected. Most notably, multi-factor authentication will incorporate one-time password (OTP) tokens, public key infrastructure (PKI) and biometrics to comply with the DEA and HIPAA for Electronic Prescription of Controlled Substances (EPCS). These solutions will also be used to protect patient records and data; provide secure access to facilities; authenticate remotely to VPNs using mobile devices; and allow for new IoT use cases. In addition, unified platforms will add intelligent visitor management systems and automate other manual processes to provide an access management solution that integrates with access control, IT security and other applications.

The second trend is the establishment of connected environments to drive the need to access the internet of trusted things (IoTT). The continued adoption of electronic visit verification (EVV) will streamline in-home patient visits and prevent billing fraud using “proof of presence” applications that document the time, location and accurate delivery of prescribed care. Healthcare providers will increasingly use trusted IDs, predictive analytics and new IoT solutions that use real-time location-based services to connect, monitor and manage patients, mobile clinicians and staff. These solutions will also help quickly locate critical medical equipment, beds, crash carts and other medical devices by providing the missing link between physical assets and a trusted ID ecosystem.

Third, the growing role for biometrics in patient and provider authentication and EPCS applications will help ensure that the right patient is receiving the prescribed care, and that healthcare providers are authorized to manage private patient medical records. Healthcare providers will also use biometric solutions for e-prescribing to authenticate the issuer, pharmacy staff and/or the patient. Lumidigm fingerprint technology will continue to be widely adopted because of its ease of use and proven security.

HID Global expects that the healthcare industry will be impacted by these trends in 2017 and beyond as the industry increasingly transitions to identity technology in the coming years.

Headquartered in Austin, Texas, HID Global has over 2,700 employees worldwide and operates international offices which support more than 100 countries. HID Global® is an ASSA ABLOY Group brand.

BIO-key

BIO-key provides fingerprint sensors and biometric software to healthcare and other industries.

The company’s core software engine is WEB-key, which delivers multi-modal authentication via an SDK. It also offers Vector Segment Technology (VST), a highly accurate and scalable fingerprint system for Microsoft Windows, and ID Director, which delivers biometric authentication in the native environment, and is available for healthcare EHR platforms.

BIO-key provides healthcare organizations with its NIST tested interoperable software and FIPS-compliant fingerprint readers for online security, workflow, and end-user convenience benefits. The company’s technologies also meet DEA and State Board of Pharmacy regulatory standards. Its solutions protect patient record and medications access, and provide efficient and compliant two-factor authentication for EPCS.

Healthcare industry customers of BIO-key include Cleveland Clinic, Nationwide Children’s Hospital, and Genesis Health Systems.

BIO-key has formed strategic partnerships to create a global ecosystem for mobile authentication with companies including mobile technology developer InterDigital, NEXT Biometrics, and IDEX, as well as security infrastructure providers such as IBM, CA, and Oracle.

BIO-key traces its roots back to 1993, when it introduced its first fingerprint algorithm. The company went public on OTC Markets in 2003. Based in Wall, New Jersey, BIO-key also has U.S. offices in Minnesota and Massachusetts, and international offices in Hong Kong and China.

GenKey

GenKey provides large-scale biometric identity management solutions for uses including elections and digital healthcare. The company provides a full identification solution, including fingerprint enrolment software, database management, and a verification solution.

GenKey stores biometric data as BioHASH templates, using a proprietary one-way encryption operation to provide data security, while also allowing offline verification. BioHASH is compliant with the ISO/IEC 24745 standard for biometric data privacy and security.

The company's BioFinger SDK has received NIST MINEX and PFTII certification for performance and interoperability, and its fingerprint image exchange algorithm meets the FBI's WSQ certification and accuracy requirements. It also provides an Automated Biometric Identification System (ABIS), which it released a new version of in early 2017, introducing a label independent matching (LIM) function to detect duplicate fingerprints, among other upgrades.

GenKey's healthcare customers include the National Hospital Insurance Fund (NHIF) of Kenya, and Ghana's National Health Insurance Scheme.

The company's biometrics-based healthcare solution was shortlisted for the "Solutions of the Year Award" in the technology and solutions providers operating in or exporting to Africa category of the 2016 Africa Healthcare Awards.

GenKey holds 39 patents. It was founded in 2001, and is based in Eindhoven, the Netherlands.

ImageWare

ImageWare Systems is a developer of identity management products, specializing in multi-modal biometrics for mobile, healthcare, financial, and enterprise markets.

GoVerifyID, the company's flagship mobile and cloud multi-modal biometric authentication service, is among ImageWare solutions providing credentialing to healthcare companies. Integrated IT solutions firm CDW partnered with ImageWare to offer its customers GoVerifyID and the CloudID product suite in late 2015.

The company announced a partnership in late 2016 with medical professionals and investors group American Biometric Solutions to market ImageWare's pillphone. Pillphone is a biometrically secured mobile healthcare communications application, powered by ImageWare GoMobile Interactive, which provides interactive medication adherence reminders and information exchange for healthcare payers, providers, and patients.

Other offerings from ImageWare for the healthcare market include photo IDs for employees and members, confidential record protection, access control for facilities and systems, employee attendance and time tracking, and biometric security for mHealth apps. The company also formed several other partnerships in 2016, including agreements with Fortscale Security, Fujitsu, and SAP HANA.

ImageWare holds 20 patents related to multi-modal biometric technology, with 14 pending. It is publicly traded on OTC Markets, with market capitalization of over $100 million, and trailing twelve months revenue of $3.79 million. The company is based in San Antonio, Texas, with offices in Portland, Oregon, Ottawa, Canada, and Mexico City, Mexico.

Imprivata (PatientSecure)

Healthcare IT security company Imprivata provides the PatientSecure biometric identification system for patient registration and identification. PatientSecure uses palm vein recognition for accurate, non-intrusive 1:1 positive patient identification.

Impravata PatientSecure integrates with major EMR programs, ADT and EMPI systems and HIS applications, as well as patient self-service kiosks from Epic, Welcome, Vecna, Connected Technology Solutions (CTS), and other providers.

Impravata also offers multifactor authentication platform Confirm ID for centralizing identification across workflows, including remote access, EPCS, medical device access, and a variety of clinical workflows. Confirm ID launched in 2015, and was significantly expanded in 2016. It manages identities by using Hands Free Authentication, push token notification, fingerprint biometrics, and other methods.

The company also provides Imprivata OneSign for single sign-on access management, and Imprivata Cortext for secure collaboration between clinician teams and organizations. The Impravata Developer Program enables SaaS, software, and hardware companies to integrate its technology, and it supports dozens of reseller partners.

Customers of PatientSecure and Imprivata's other biometric solutions include Carolinas HealthCare System, BayCare Health Systems, Adventist Health System, and Baton Rouge General Medical Center.

Impravata was founded in 2002 and is based in Lexington, Massachusetts.

Intelligent Fingerprinting

Intelligent Fingerprinting provides a mobile, non-invasive drug screening system based on analysis of fingerprint sweat, a patented diagnostic technique.

The system consists of the Intelligent Fingerprint Reader 1000 and single-use collection cartridges. The reader uses proprietary immunoassay reagents to analyze sweat, and does not require specialist collection or handling services, unlike other screening methods. Sample collection takes less than five seconds, and testing for multiple drug groups takes less than 10 minutes.

A version of the reader which confirms the identity of the person providing the sample using their fingerprint is in development.

The system allows samples to be tested immediately or retained in tamper-proof cartridges for later testing, and also allows drug detection cutoff levels to be customized. The test identifies drugs of abuse in four groups: amphetamines, cannabis, cocaine, and opiates.

Intelligent Fingerprinting is ISO 13485 accredited for its quality management system for medical device design and manufacture.

The company raised over $3.5 million in funding in 2016 to bring it to approximately $12.6 million in private investment, in addition to several government-funded grants. Grant awards include funding for pilot studies with the UK National Health Service and coroners.

Intent Solutions

Intent Solutions is a technology, software, and data services company serving the healthcare industry.

It provides the TAD (Take as Directed) mobile smart medication dispenser, which uses fingerprint authentication to prevent the misuse and diversion of prescription medications, and improve health outcomes. TAD is being used in a pilot project by MAP Health Management, announced in February 2017, to track compliance with medication protocols by patients with substance abuse disorders.

Along with the TAD device, Intent Solutions offers a mobile app and a real-time virtual database for monitoring and managing behavioral and adherence data.

Intent Solutions collaborates with the Alliance for Adoption of Innovations in Medicine (Aimed Alliance), a U.S. not-for-profit organization seeking to improve healthcare through access to evidenced-based treatments and technologies.

Intent Solutions was founded in 2013, and is based in Atlanta, Georgia.

IriTech

IriTech provides hardware, software iris recognition products, as well as cloud and mobile solutions.

The company's hardware products are the IriShield Series of iris scanners sold in cases or as modules, and the Gemini Camera, which captures face and dual iris at the same time with a single CMOS sensor. It also provides the IriCore iris recognition SDK for Windows and Linux, along with the IrisCoreLite API library, IriMaster middleware server software, and other software products.

IriTech provides the healthcare industry with a patient-identification solution which includes patient registration and tracking for treatments, different departments, and checkup arrangement. The solution supports national or private health insurance cards, ambulant treatment documents, wrist bands, and iris biometric identification.

Following a successful pilot at Arrixaca Hospital in Murcia, Spain in 2016, biometric identification provider Umanick is promoting IriTech's mobile iris recognition solution, which uses IriShield cameras, in the Spanish healthcare market.

The company has strategic partnerships with Lockheed Martin, Texas Instruments, Aware, Accenture, CSC, NEC, the FIDO Alliance, and others. Its clients include government projects in the U.S., India, Kenya, and Thailand, military projects for the U.S. Military and Department of Homeland Security and Lockheed Martin, and UN refugee programs in Malawi and Thailand.

IriTech was founded in 2000, and is based in Fairfax, Virginia. It has regional offices in Korea, Japan, Vietnam, Russia, and India.

M2SYS/RightPatient

RightPatient is the healthcare industry brand of M2SYS, providing a multi-modal biometric patient identity platform. It is offered as a SaaS solution, integrated with the electronic health records (EHR) system, and providing back-end data storage and matching in its HIPAA-compliant cloud.

Interfaces are available from RightPatient for EHR systems including Epic, Cerner, McKesson, Meditech, and CPSI. The platform is capable of authenticating patients with fingerprint, finger vein, palm vein, iris, facial, and voice biometrics.

RightPatient EMPI interfaces with any master data management (MDM) system for real-time patient identification from any service delivery location. RightPatient also provides the PatientLens facial recognition software for mobile devices.

RightPatient RemoteID enables secure access to PHI data via mobile healthcare apps with facial or voice verification. RightPatient Global Connect provides biometrically secured federated patient identities, leveraging the RightPatient cloud.

M2SYS Technology is a biometric software and scanner provider, with a focus on removing the friction from the development and deployment of identity management solutions.

M2SYS' other products include the CloudApper dynamic cloud application framework, the CloudABIS biometric-as-a-service (BaaS) system, and the Bio-Plugin SDK, which allows developers to integrate multi-modal biometric software with less development work than other SDKs.

M2SYS was founded in 2002. RightPatient was founded in 2011, and along with the rest of M2SYS is based in Atlanta, Georgia.

MedixSafe

MedixSafe provides storage and access control devices for controlled substances, enabling fingerprint, proximity card, and IP-based remote management of narcotics dispensing. It also introduced facial detection and capture capabilities in 2016.

The company's cabinets, lockers, and safes provide medicinal inventory tracking and automated record keeping to increase accountability and compliance and to provide an audit trail for authorities such as the DEA. Its dozen different products include specific offerings with different sizes and features for use in ambulances, wall mountings, and small pharmacies and clinics.

MedixSafe's target market is healthcare providers with a need to secure and track access to controlled substances by staff to prevent theft and substance abuse.

Customers of the company include agencies and businesses in 44 states, four Canadian provinces, Saudi Arabia, and the United Arab Emirates. MedixSafe was founded in 2009 by Memphis-based electronic security and network cable company Electronic Security Specialists (ESSC, Inc.).

NextGate

Healthcare data management company NextGate provides an Enterprise Master Patient Index (EMPI), which is built on the MatchMetrix master identity platform, and features facial recognition, which was added to MatchMetrix in September, 2016.

It also offers a Provider and Organization Registry, Cross-Enterprise Document Sharing (XDS) solutions, and an Intelligent Data Aggregation Server (iDAS).

NextGate's EMPI facial recognition capability improves record matching accuracy and allows patient self-registration. It works with available cameras, such as those embedded in tablets smartphones, and in addition to integration with the NextGate EMPI, can be configured for deployment on existing infrastructure in various environments. Its facial recognition technology is offered as a vendor-neutral software solution providing two-factor authentication, and use with mobile devices. NextGate says that it provides faster patient registration, increased matching accuracy to patients and to patient data exchanged between systems, eliminates duplicate record creation, and flags fraudulent activity.

NextGate partners with IT vendors and system integrators, such as Accreon, Caradigm, CSC, GE Healthcare, Infor Healthcare, MatrixCare, and Novarad. Healthcare organizations served by NextGate include health insurance providers, health information exchanges, health systems and integrated delivery networks, provider groups, and specialty practices, with clients among National Health Services (NHS) boards in the UK and medical service and information groups in the U.S.

The company was founded in 2005, and is based in Pasadena, California.

Rx Safes

Rx Safes is a fingerprint medical device and security storage company. It designs, develops, engineers, and markets solutions to regulate and secure controlled substances at the patient and consumer level. Rx Safes is a GeneSYS-RX company.

Products offered by the company include Rx-SafeDOSE PCA infusion pump regulators, Rx MyDOSE needleless injectors, and the Rx DrugSAFE line of security and storage products for consumers and healthcare professionals, all utilizing biometric authentication. Rx Safes products are designed for hospitals, emergency service providers, healthcare workers, assisted living facilities, and nursing facilities.

Rx Safes also offers the Rx SafeEHR, a HIPAA-compliant portable storage device secured by onboard fingerprint matching, and the Rx DrugSAFE FieldLOCK to secure field kits for EMS, ambulance, and paramedic crews. Rx Safes has six additional products in development, including a Mobile Medical Station (MMS) to support the Affordable Care Act's "Health Home" model, an organ transportation case, and a safe for prescription medications in the consumer's home.

The company's proprietary fingerprint technology for the healthcare market measures several layers through the skin. It then converts the measurements into a personal code for enrolment and subsequent matching.

Talon Brands became the preferred distributor of Rx Safes' products in North America with a licensing agreement in 2016.

GeneSYS-RX and RX Safes were founded in 2010, and are based in Henderson, Nevada. The company stated a commitment in 2016 to meeting the listing requirements for the NASDAQ Capital Markets.

Safran Identity & Security

Safran Identity & Security (formerly known as Morpho) is a global security and identity solutions vendor, providing biometric terminals and products for civil and commercial identity and public security.

The company specializes in fingerprint, facial, and iris recognition, and uses vein and multi-modal recognition. It offers portable terminals, sensors, software, mobile applications, and automated control gates.

Safran Identity & Security's modular healthcare identification solution is based on a biometric smart card for use by both patients and healthcare professionals. Safran Identity & Security's Card Management System (CMS) has been deployed to issue more than 33 million e-health cards (eGKs) to help modernize the German healthcare system.

Safran consolidated its companies' names in May, 2016, to bring them under the single brand "Safran." Morpho, which had been the group's security and identity company, became Safran Identity & Security. Private equity investor Advent International subsequently reached a deal to acquire a majority share of the company from Safran for €2.425 billion (US$2.59 billion) in September, 2016.

Other companies within the Safran group also provide biometric services to the healthcare market, including MorphoTrust USA (Safran)'s Trusted Identity-as-a-Service (TIaaS).

Safran Identity & Security was founded as Morpho in 2007. The company is based in Issy-les-Moulineaux, France, and has 8,900 employees in 62 countries, serving more than 100 national markets. It generated nearly €1.9 billion in revenue in 2016.

Simprints

Simprints is a non-profit company which builds low-cost, durable fingerprint scanners to provide to front-line workers for non-governmental organizations (NGOs) and government agencies working to create formal identification for people in under-served communities to fight poverty by enabling access to essential services. It seeks to improve healthcare delivery by allowing health workers to access patient medical records at any time or place.

The company uses open-source software and proprietary hardware based on research by Simprints personnel at the University of Cambridge. The scanner is mobile, using Bluetooth connectivity, with an ergonomic handheld design. It a long-lasting battery and water-resistant casing, and Simprints says it is 228 percent more accurate than existing mobile scanners in low-resource settings.

Simprints is compatible with Web and Android 3.4 or later-based applications, with standard Android calls and a cloud-based RESTful API. The company says its cloud platform allows IDs to be securely synced across devices, and allows integration with nearly any mobile data system.

Simprints healthcare projects include working with development NGO BRAC in impoverished areas of Dhaka to improve access to maternal healthcare, and a partnership with VaxTrac in Benin to design systems for better vaccination coverage.

Simprints was founded in 2013 and is based in Cambridge, England.

Medical Biometrics

In contrast to healthcare 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 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. Such devices will be able to provide medical diagnostic data through internet-based cloud applications in the near-term.

Biometrics Research Group, Inc. believes that "medical biometrics" will continue to develop into a growth market due to increasing demand for "wearable" consumer electronics. The increasing use of mHealth applications will also drive the utilization of biometric authentication for security purposes.

In a previous research note issued by Biometrics Research Group, 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, such as 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 health and the practice of medicine. The result is the emergence of wearable and even ingestible sensors.

IDTechEx, a market research firm, has projected that the market for wearables was worth over US$30 billion in 2016, and will grow in three stages: 10 percent annually to over US$40 billion in 2018, but then accelerating to 23 percent to over US$100 billion by 2023, before slowing to 11 percent and surpassing US$150 billion by 2026.

As reported previously in BiometricUpdate.com, a wide range of other biometric fitness and healthcare applications continue to enter 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. By capturing objective information and providing actionable insights, patients using the technology can take control, communicate with caregivers and clinicians, and improve their health. Such sensors, when taken alongside medications, will be powered by the body's biochemistry.

With an explosion of new biorhythm monitoring technologies, Biometric Research Group, Inc. expected the biorhythm monitoring market to reach US$100 million in sales by 2015, thereby enhancing the bottom line for consumer electronics retailers. Indeed, wearable computing continues to be a key highlight of the consumer technology industry.

Mobile health, also known as mHealth, will also be a major driver for the medical biometrics market segment. 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 the use of 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 by 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 receives significant media attention, and device manufacturers such as Apple and Samsung 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.

Conclusion

In the healthcare sector, biometrics are mostly 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. expects the use of biometrics to accelerate through the entire global healthcare sector due to the expanded adoption of biometrics to enhance cost saving methods to combat fraud in both government-insured programs and private sector insurance marketplaces. Growth in the use of biometrics in the sector will primarily be driven by the continuance of healthcare reform through legislative repeal and replacement in the U.S., which will be mainly driven by cost containment imperatives. Medical biometrics, led by mHealth and wearables, will continue to make in-roads in the consumer technology marketplace.