IBIA

Program Integrity White Paper
DRIVING REDUCTION IN HEALTHCARE FRAUD WITH BIOMETRIC IDENTITY

Submitted by the

International Biometrics & Identification Association (IBIA)

Introduction

In response to your solicitation "for ideas from all interested stakeholders in the health care community regarding solutions and suggestions for how to better prevent and combat the multi-billion dollar problem of waste, fraud, and abuse in the Medicare and Medicaid programs, the International Biometrics & Identification Association (IBIA) is pleased to submit these comments on the important role that biometric solutions can play in reducing waste and fraud within the systems as well as in enhancing quality health and system efficiencies. IBIA appreciates the opportunity to contribute to this important effort to sustain the long-term viability of these key programs.

IBIA is a non-profit trade group based in Washington, DC**.** The attached brochure outlines IBIA's current mission, activities, and recent track record. It also lists the IBIA members and the Board of Directors.

The key focus of IBIA is the use of technology in determining identity and promoting the effective and appropriate use of technology to determine identity and enhance security, privacy, productivity, prevention of fraud, and convenience for government, the commercial sector, and consumers.

Identity plays a vital role in our globally connected world and biometrics is one of the technologies that plays an increasingly important role in the identification of individuals, with its use reaching into our everyday lives. Biometrics is commonly embedded in military and intelligence activities as well as in solutions that protect national borders and ports; enhance programs like driver's licenses and social benefits registrations; secure facilities like daycare centers, banks, health clubs, and schools; prevention of identity theft; secure data and transactions for financial and health care institutions; and protect personal data in laptops and mobile devices.

To carry out its mission, IBIA engages in policy advocacy at the federal and state levels, education outreach, and provides a dialogue center for exchanging information and ideas. IBIA's activities focus on both the government market and the commercial /consumer sectors.

Executive Summary

The International Biometrics & Identification Association (IBIA) proposes the inclusion of a biometric-based solution in your efforts to address the waste, fraud, and abuse challenges in the Medicare and Medicaid programs.

A biometric-based solution provides significant benefits for program integrity by deterring fraud. The benefits of a biometric solution, however, go well beyond deterring fraud and include other significant benefits – including improved patient health care quality, safety, and privacy and increased efficiencies in the programs.

This is because a biometric solution is the only system available today that provides positive identity of an individual with a high level of assurance. No other solution provides the same "degree of certainty" of “knowing who" as does a biometric solution.

In matters of fraud and identity theft, it is always the “who” that is important. It is never the system, card, token, password, PIN or system that misbehaves. It is always (100%) an unauthorized and ill-intentioned individual who is at the heart of every fraudulent attack or issue.

The basic problem is to determine “who” with a high degree of certainty. A biometric-based solution provides this high “degree of certainty” of “who” because it is based on unique physical traits of individuals and is not dependent on breeder documents that can be forged or altered.

Biometric solutions today are proven, reliable, widespread in the U.S. and globally, easy to use, and convenient. They are also in widespread use in the U.S. and globally and have a high degree of public acceptance.

The remainder of this paper describes in detail

- How a biometric-based solution works
- How the biometric solution functions to deter fraud and enhance patient health care quality, safety, and privacy
- The widespread use and acceptance of biometric solutions in the U.S. and globally
- Rebuttals to misconceptions about biometric solutions
- Successful case studies of biometric solutions in private sector health care settings

Benefits of a Biometric Solution

In matters of fraud and identity theft, it is always the "who" that is important. It is never the system, card, token, password, PIN or system that misbehaves. It is always (100%) an unauthorized and ill-intentioned individual who is at the heart of every fraudulent attack or issue.

The basic problem is to determine “who” with a high degree of certainty. A biometric solution is the only system available today that provides positive identity of an individual with a high level of assurance. No other solution provides the same "degree of certainty" of “knowing who" as does a biometric solution.

The benefits of “knowing who” include deterring and preventing fraud. The benefits of “knowing who”, however, go well beyond deterring fraud. It also leads to other significant benefits by virtue of its ability to immediately authenticate an identity – including better health care and more efficiency in the system that further increases overall system savings.

A biometric-based solution provides this high “degree of certainty” of “who” because it is based on unique physical traits of individuals. This is how it works.

What distinguishes a biometric-based system.

A primary goal of any identity system is to ensure that there is only one identity for every person in the system, in other words, that every name in a system is associated with a single person.

An identity system cannot be based on names alone. Experience has shown that names are often duplicated in a population and, therefore, other information is required to secure a unique association with an individual, such as date of birth, address, height, weight, etc. Usually the source of this other information, however, is dependent on the word of the individual or other documents that the individual presents. These breeder documents can be forged or altered and do not provide the basis for a reliable identity system.

A biometric-based system, however, ensures the integrity of each identity in the system because it is using information that is unique to that individual, consistent and immutable for life, and not dependent on breeder documents that can be forged or altered.

Because a person’s biometrics are considered unique and are permanently associated with an individual, coupling a biometric to a name of a person in the identity system assures the uniqueness of the individuals within the system, independent of any forged or altered document or statements. The system can then be used to confirm the identity of the person or to self-search to determine duplication of an enrollment.

In addition, since a biometric-based system does not require any additional information to confirm a claimed identity, once a person is enrolled into the system, that person's identity can be confirmed merely by providing his/her biometric. This patient convenience eliminates the need for potentially altered or forged documents such as drivers' license, an identity card, a flash pass, etc.

<u>Biometric solutions are the most effective solutions for preventing a fraud from being perpetrated in the first instance.</u>

Fraud deterrence is a crucial part of any effort to reduce waste, fraud, and abuse. Deterrence is by far more cost-effective than trying to recover erroneous payments, which are rarely recovered in full in either fee-for-service or managed care programs. Deterrence is also likely to reduce overall program costs because it mitigates the need and cost of hiring contractors and auditors.

The current systems – pay & chase as well as predictive analytics – do not deter fraud. Pay & chase is used to "recover" improper or fraudulent systems and comes into play after the service, benefit, or medications etc. have been provided and after payments have been issued. Predictive analytics is also applied after the fact to identify questionable patterns of behavior for closer scrutiny of individuals in the future. Both systems are costly, requiring contractors and auditors to sift through voluminous claims data, and produce limited success in actual recovery. In a very costly and lengthy process, it also requires an examination of individuals' medical records on a case-by-case basis to prove an improper payment and make a recovery for that specific incident.

By way of contrast, a biometric solution deters the fraud at the outset, before enrollment and services and benefits are provided and it is the only method available that functions as a deterrent.

The biometric solution serves as a deterrent because, being based on the unique trait of the patient, it is possible to determine immediately with a high degree of certainty "who" is attempting to enroll or is requesting benefits or services.

Multiple enrollments of the same person under different names are identified immediately because the biometric presented is already in the system under a specific name, thus preventing multiple benefits to the same individual.

If services are requested by an individual under a name in the system but whose biometric is different from the biometric already in the system that is associated with that name, it will be immediately identified and rejected.

In effect, after a period of time, people are deterred from trying to "game" the system because they learn that there is too much risk associated with doing so.

Use of biometric solutions to secure patient and provider identities can prevent certain health care fraud.

Biometric solutions deter and reduce fraud in numerous important respects.

- Ensure that people do not possess multiple fraudulent identities in order to obtain duplicate benefits, drugs, and services. No other technology can do this. Duplicate enrollment is becoming an increasing problem in the Medicaid program. Because it is based on unique personal characteristics, biometric identity is the most effective means for determining whether an individual applying for benefits is already receiving those benefits under a different name. It will also prevent others from enrolling under a name that is associated with a biometric already in the system, either through theft of an identity or collusion with a participant in the program.
- Deter and prevent card sharing and patient identity theft by validating the patient's physical presence in the provider's location on a given date. The recently-released 3rd annual Experion /Ponemon medical identity theft survey concludes that a significant amount of fraud results from people sharing medical and insurance information with friends and relatives.
- In fee-for-service programs, prevent the provider from billing for "phantom claims" or services by validating the patient's physical presence at the provider location on the service date. The vast amount of fraud associated with phantom claims can only be prevented by validating a patient's presence for service.
- Facilitate compliance with privacy regulations like the Health Insurance Portability and Accountability Act (HIPAA) by preventing unauthorized access and establishing a log of access events.
- Create an "audit trail" of check-in and check-out times for comparison against type of service provided as an indicator of potential fraud called "upcoding".
- Verify managed care "encounter data" or services from providers so that Medicare and Medicaid programs can rely on this reported data for the setting of managed care rates.
- Reduce inventory loss and theft, for example, by securing medication cabinets through biometric access, which provides an audit trail detailing who accessed the inventory or requiring a biometric signature by the patient for proof of receipt of durable medical equipment and supplies.

Biometric-based solutions also improve health care quality, safety, patient privacy and deters medical identity theft.

"Knowing who" with a high degree of certainty means higher quality patient health care services, safety, and privacy. These are consequential issues to patients and, contrary to the misperception that a biometric solution takes advantage of a vulnerable population, the biometric solution enhances their health care quality, safety, and privacy.

Biometric solutions

- Ensure correct identification of the patient and matching him or her to the proper record during admission. This is particularly beneficial in emergency situations where the patient is confused or unresponsive, and treatment must begin immediately. In addition, RFID and barcode bracelets can be purposefully swapped or accidentally applied to the wrong patient, resulting in improper treatment.
- Increase patient safety by reducing medical risks, accidents, and errors due to mismatched or incomplete records.
- Prevent accidental or purposeful misidentification leading to blending of two or more histories into one record.
- Protect patient identity and patient health care information by providing an efficient and convenient means of authenticating both patients and providers before allowing access to records.
- Provide a unique and more accurate patient and provider master index to ensure that patient records in multiple provider locations can be linked accurately, increasing the usefulness of electronic health records, their safety, and privacy.
- Enhance privacy because patients will no longer need to rely on paper cards with personally identifiable information, like name, date of birth, and social security numbers, which can easily be lost or stolen or forgotten.
- Deter medical identity theft, a major problem as demonstrated in the recently released Experian /Ponemon poll on medical identity theft. For example, according to the report, more than half of the people surveyed were victims of medical identity theft. Of the victims, half failed to report the theft and had to pay their health care providers out-of-pocket. Extrapolating from the data they had, the authors estimated that the cost per year of those payments is *$41 billion*. The biometric solution will prevent anyone other than the eligible patient from accessing the system under the name of an existing patient.

<u>Biometric-based solutions also facilitate increased process efficiency.</u>

“Knowing who” with a high degree of certainty also increases efficiency within a system, thereby further contributing to program savings.

- Because the biometric solution to “know who” is automated, contractors and auditors no longer need to manually search and verify records for providers or participants. This reduces the costs associated with oversight of fraud prevention programs, as well as the waiting periods for beneficiaries.

- By preventing or deterring fraud, it reduces the costs and risks associated with the "pay & chase" programs that attempt to recoup fraudulent payments after the fact, often based on inaccurate data.
- It increases efficiency on the provider side because there are fewer forms to fill out, fewer clerical errors, and enables speedier billing and payment.
- It simplifies the process. Most security systems and technologies are overly complex by design. They are intended to block, not enable. Biometrics solutions, designed correctly, are intended to enable access and are more like a guardrail than a barrier. Thus, biometric-based solutions have the unique benefit of being both secure and convenient.

Misconceptions about the use of a biometric-based solution do not withstand scrutiny

Notwithstanding the increasing use and acceptance of biometric-based solutions in the U.S. and globally, negative perceptions and lack of understanding about the reliability and the positive benefits of biometric solutions linger in certain contexts, such as, in the Medicare and Medicaid programs.

Contrary to these misperceptions, however, biometric solutions are proven to be effective and reliable and are in widespread use globally in numerous and different ways. *(Please see the attached memorandum that summarizes just some of the biometric solutions in use around the world today.)* Biometric solutions are also widely used specifically in the private health care sector where they have proven successful as well as popular with providers and patients alike. *(Please see attached case studies and the discussion below).*

<u>Use and acceptance of biometric solutions are widespread today.</u>

Use of biometrics by government, the commercial sector, and individual consumers has become widespread for many useful purposes: to prevent cheats from using stand-ins to take professional competency and academic admission examinations; in school lunch programs to avoid bullying for lunch money and to avoid stigmatizing low-income children who receive food benefits; in day care centers to match parents with children to prevent kidnapping; to protect against unauthorized access to sensitive financial, health, and other data in information systems; and to protect facilities against unauthorized access. It is used for logical and physical access, for background checks to obtain a variety of licenses such as real estate, brokers, drivers, and other professionals, even for identity management in the Armed Forces.

There is no stigma associated with the use of biometrics. American citizens understand that biometric solutions serve beneficial purposes and protect privacy and identity. If there is no stigma to a member of DOD protecting our country, to a school child receiving food through a lunch program, or a gym member accessing facilities, there is certainly no stigma for Medicare and Medicaid clients.

According to the latest Unisys Security Index report conducted in October 2010, national security and identity theft rank as America's top concerns, with 64% seriously concerned about identity theft. http://www.unisys.com/unisys/news/detail.jsp?id=1120000970006010116.

Biometric solutions protect privacy.

Biometric data is less vulnerable to jeopardizing privacy than personally identifiable information (PII) that are routinely saved on databases.

The biometric database is comprised of "templates" and not the biometric images. A template is a series of digital representations of the image and not the actual image. If a breach of a biometric database occurs, the breach would only yield pieces of data that are virtually impossible to reverse engineer. Furthermore, there is little that can be done with this digital data because that person does not have your unique biometric. This is unlike what happens when someone acquires your PII – name, address, date of birth, social security number. This information can be used to steal your identity and create a host of financial and legal problems.

Biometric enrollment is not a barrier to access to Medicare and Medicaid.

A common objection to a biometric solution is that the enrollment process will be a barrier to program access by virtue of the logistics involved, such as difficulties in getting to enrollment centers.

However, there does not appear to be any evidence that this is the case. In the only Medicaid biometric pilot done to date (in Texas), biometric enrollment was done by the client at the initial visit to a provider's location – after the client had already been determined to be eligible and had received notice of eligibility status. The biometric enrollment at the provider location took 2-3 minutes and a client's second visit to this provider or another only required the authentication of the biometric, a process that took seconds. It is anticipated that that any health care biometric enrollment in Medicaid or Medicare could work similarly.

In addition, mobile technology facilitates the ability to enroll patients in virtually anywhere and at anytime – in nursing homes, at home, in hospitals, in clinics, and other remote locations. The enrollment process is simple and short and it requires minimal assistance and training from providers and staff on the enrollment process.

Costs of biometric solutions have gone way down.

A common objection is that a biometric-based solution may be too costly is not borne out by the facts. Costs of biometric systems have decreased dramatically while performance has gone way up, and reliability has increased to a level where it is possible to deal with a broad and diverse population.

Implementing a biometric solution would function no differently than any other technological add-on, such as new encryption software or new anti-virus software. Aside from the acquisition of the scanners and readers, implementing biometric solutions would make use of existing computer technologies and personnel. As a result, the upfront costs associated with adopting a biometric solution would be minimal in comparison to the costs to administer the overall Medicaid or Medicare programs.

It is difficult to estimate the specific cost of a biometric solution without knowing the specific system design. Systems can be designed in a variety of different ways to accommodate the needs involved. That decision will impact the cost.

A system can be designed to use a smart card, fob, mobile device for storing and matching purposes or none at all where matching is done on a server.

A system that uses a smart card or other device will likely cost more up front than a system that uses matching on the server. Administrative costs could also be higher because of the need to replace the stolen or lost cards or devices.

On the other hand, there are factors other than costs that may be relevant in designing a system. People may feel more secure about their privacy with a card or device that holds their personal data rather than have the data stored on a database.

For others, securing data in a database on a server is not a concern (a database will always be needed for enrollment purposes). It may be more important not to have to rely on a card or device that can be lost, forgotten, or stolen. This is particularly relevant for the elderly or when emergency care is needed immediately and patients are confused or unresponsive.

These are all factors that will determine costs and why it is essential to conduct projects, mandatory phased trials and pilots on the major options to get the information needed to make informed decisions that could clearly show the monetary savings, the most effective ways of using a biometric-based solution in Medicaid and Medicare, and other important benefits of a biometric solution.

Case studies of health care projects in the private sector

Biometric-based solutions are making major inroads in the private health care sector.

The attached document provides a number of case studies and also lists numerous health care facilities that use biometric solutions but have not written up case studies.

In addition, there are several large scale systems in the U.S. and internationally that are reluctant to go public at this time for a variety of reasons but have talked to IBIA about their projects.

All these diverse examples share similar goals:

- **Reduce runaway waste, fraud, and abuse**
- **Improve patient safety and convenience**
- **Protect against identity theft**
- **Ensure accuracy of medical records**

The following additional examples of biometric solutions in health care settings, with descriptions of resulting benefits, were cited in the Virginia Medicaid Biometric Pilot Implementation Report, prepared by the VA Department of Medical Assistance Services pursuant to state legislation authorizing a biometric solution in Medicaid. (The Virginia pilot has still not been undertaken.)

- A hospital system in Kentucky uses fingerprints for patient identification
- A health clinic in New York City serving both uninsured and Medicaid patients uses photographs and iris recognition for patient identification and medical records management. According to the report, the technology, located in all reception and examination areas, has enhanced quality of care by identifying and matching specific patients to their EMRs, eliminating duplicate medical records for patients who give alternate versions of their names during registration, and reducing opportunities for insurance fraud by individuals attempting to obtain benefits belonging to others.
- Florida Medicaid recently implemented a voice recognition biometric pilot in the Miami-Dade County Area to prevent home health care fraud by requiring providers to contact the state to verify that they actually delivered services to recipients in their homes.
- Hospital systems in California and Florida use palm vein recognition in hospital reception areas for immediate identification and registration as well as in emergency departments to identify patients who are unconscious or delirious.

The success of these projects has been stunning, with high degrees of satisfaction and acceptance from both the health care providers and the patients. *(Please review the attached case studies.)*

Conclusion

Thank you for this opportunity to present the case for the use of a biometric-based solution in government efforts to deter and reduce waste, fraud, and abuse in the Medicare and Medicaid programs.

In summary, the case for the use of a biometric solution in the Medicare and Medicaid programs is straightforward: it provides positive benefits for program integrity by deterring fraud and also benefits patients by improving their health care quality, safety, and privacy:

- Fraud deterrence must be a crucial part of government efforts to reduce waste, fraud, and abuse and a biometric solution is the most effective tool available for deterring the fraud from being perpetrated in the first instance.
- The benefits of a biometric solution go way beyond fraud deterrence program to enhance the quality of patient health care services, safety, and privacy and protect patients from medical identity theft, in sharp contrast to the misperception that a biometric solution in these programs takes advantage of a vulnerable population. These are important benefits that increase the satisfaction of program participants and the smooth, efficient, and cost-effective functioning of the Medicare and Medicaid programs – in short, program integrity in the broadest sense.
- The biometric solution also simplifies and rationalizes program processes.
- No other system provides these crucial program integrity, patient, and process benefits.
- Biometric solutions are proven, reliable, easy to use, and convenient. They are also in widespread use in the U.S. and globally and have a high degree of public acceptance.

For these reasons, IBIA very much hopes that you will support a biometric solution as a key tool in government efforts to deter waste, fraud, and abuse in the Medicare and Medicaid programs.

To assist in your efforts to understand how a biometric solution works, IBIA would recommend the following:

- Support mandatory broad-based and phased trials and pilots to obtain the cost and technical information needed to make informed decisions on implementing biometric solutions. It is important that these efforts are mandatory. It is not possible to show cost savings on the basis of a limited pilot. (This was the problem with the pilot in Texas and led CMS to conclude the pilot had not shown that the biometric solution was cost-effective and curtailed fraud. Because it was voluntary, anyone intent in committing fraud would go to providers not involved in the pilot. Participants also did not see benefits because the biometric card was used in addition to the regular paper registration.)

  All patients and providers in an area have to participate regardless of where they receive services to be able to get relevant information.

- Support public education to help people to understand the purposes and benefits of a biometric solution and how the system works. This will facilitate getting the most information out of the trials and pilots so that they are most useful. As significantly, it will enhance public acceptance.

The IBIA Board of Directors would appreciate the opportunity to meet with you at your convenience to answer questions and to discuss the potential role for a biometric solution in Medicare and Medicaid.