REPORT OF THE DEPARTMENT OF MEDICAL ASSISTANCE SERVICES

Virginia Medicaid Biometric Pilot Implementation Report

TO THE GOVERNOR AND THE GENERAL ASSEMBLY OF VIRGINIA

HOUSE DOCUMENT NO. 10

COMMONWEALTH OF VIRGINIA
RICHMOND 2010

Virginia Medicaid
Biometric Pilot Implementation Report

Department of Medical Assistance Services

November 2010

Executive Summary

Biometrics is the science of identifying people based on certain unique physical and/or behavioral characteristics. Examples of biometric identification modalities include face, fingerprint, hand, retina, iris, and walking patterns. The use of biometrics for identification is not a new concept. In fact, unique physical traits have been used to identify individuals for thousands of years. Currently, biometrics are used to identify people in many diverse settings including amusement parks, airports, public schools, hospitals, and federal government facilities. Within health care, biometrics are increasingly being used for identification due to concerns about patient safety, identity theft, and insurance fraud. The use of biometrics in health care will likely increase in the coming years as the industry shifts toward electronic medical records and other health information technologies as required under both the American Recovery and Reinvestment Act of 2009 and the Patient Protection and Affordable Care Act of 2010.

Recognizing the importance of biometrics, the 2010 General Assembly passed House Bill (HB) 1378 directing the Department of Medical Assistance Services (DMAS) to develop a biometric pilot to enhance efficiency and quality of care, while reducing waste, fraud, and abuse in the Virginia Medicaid Program. HB 1378 specifically states that the pilot is to be implemented as a mandatory program for all recipients residing in three localities and that the program is to be funded entirely using federal funds. To date, the federal government has not allocated any funding for the pilot. HB 1378 also directs DMAS to submit a report to the General Assembly outlining its plan for implementing the biometric pilot. This report fulfills that requirement and contains information on biometrics, the use of biometrics in health and human services settings, and the process that DMAS will follow to implement the biometric pilot through a competitive request for proposal process, should full federal funding become available.

Two caveats exist to HB 1378 that would affect implementation of the biometric pilot. The first caveat concerns the mandatory participation requirement. According to the Centers for Medicare and Medicaid Services, implementing the pilot as a mandatory program would represent a maintenance of effort violation under both national economic stimulus and health care reform legislation, which could cause Virginia to lose all federal funding for its Medicaid program. To prevent this from occurring, the pilot is designed as a voluntary program. The second caveat involves a cost-free health insurance eligibility and benefits initiative developed by the Virginia Health Exchange Network (VHEN). This initiative gives providers free card swipe machines that can be used to verify patients' health insurance eligibility status and to calculate their copayment charges for medical services. Implementing the biometric pilot would be hindered if providers decline to participate because they are already participating in VHEN's free eligibility and benefits initiative.

Table of Contents

Appendices

Introduction

House Bill (HB) 1378 passed by the 2010 General Assembly directs the Department of Medical Assistance Services (DMAS) to develop a plan for implementing a biometric identification pilot to improve efficiency and quality of care, while reducing waste, fraud, and abuse in the Virginia Medicaid Program (see Appendix 1). HB 1378 specifically requires that the pilot be used to verify the identity and eligibility of Medicaid recipients, while creating, storing, and using electronic records containing information about the type, nature, and duration of medical services provided to recipients. It also requires DMAS to implement the pilot as a mandatory program for all recipients residing in one urban, one suburban, and one rural locality, distribute all necessary equipment and materials to recipients and providers at no cost, and monitor/verify the accuracy of claims submitted by providers. HB 1378 also requires DMAS to ensure that all biometric devices and systems used as part of the pilot comply with biometric standards developed by the federal government and all relevant regulatory requirements related to interoperability and information security. In addition, HB 1378 requires DMAS to protect recipient personal identifying information from unauthorized disclosure, ensure that all recipients and providers are fully informed of the purposes and requirements of the pilot, demonstrate actual data capture and verification processes to every participating recipient and provider, develop procedures for addressing problems related to the theft, loss, malfunction, or damage of biometric equipment and documents provided as part of the pilot, and develop a method by which recipients and providers can contact DMAS for assistance. Finally, the legislation states that the biometric pilot would be funded entirely using federal funds, and that DMAS is not authorized to implement the pilot until it receives such funding. (The amount of funding that DMAS may receive is unknown at this time.)

HB 1378 requires DMAS to submit a plan for implementing the pilot to the General Assembly. This report serves as that plan. To collect data for the report, DMAS staff reviewed documents on biometric identification systems, interviewed staff in states that operate biometric systems for public assistance programs and at private companies that develop and/or implement biometric technologies, and attended two presentations on biometrics. The sections that follow contain information on biometric identification modalities, the use of biometrics in health and human services settings, the process for implementing a biometric pilot in Virginia Medicaid, and a recent initiative by the Virginia Health Information Exchange Network that may affect implementation of the biometric pilot.

An Overview of Biometric Modalities

Biometrics is the science of identifying or verifying the identity of people based on certain unique physiological and/or behavioral characteristics, rather than tokens such as magnetic stripe cards, medical insurance identification cards, drivers' licenses, or building access cards. Biometric systems consist of automated methods for authenticating and identifying individuals. Authentication consists of comparing

previously obtained biometric traits (or samples) from individuals enrolled in a database against newly submitted samples, while identification involves recognizing specific individuals from the entire enrolled population based on their biometric traits. For example, a database could be searched to determine if specific individuals have previously enrolled in a program using different names by comparing their biometric samples against existing samples. This is referred to as "one-to-many" matching. A biometric system can also be used to verify the identity of people based on their previously submitted samples. This is called "one-to-one" matching. The end result of either process is the generation of a match or non-match finding resulting in certain actions, such as granting or denying individuals access to services. A major benefit of biometrics is that it can be used to accurately authenticate and/or identify people without having to rely on tokens that can be lost, forged, stolen, or left at home.

Biometrics is rapidly evolving and a number of identification modalities have emerged including fingerprint, facial, voice, hand geometry, palm vein, signature, retina, iris, keystroke dynamics, walking patterns, and DNA analysis. There is no one best modality for all situations and many factors must be considered before implementing a biometric system. For example, one factor to consider is whether sufficient evidence exists supporting the accuracy of a particular biometric modality. Considerable research supports the use of older biometrics, such as fingerprints; however, newer modalities, such as palm vein, may require additional research before their accuracy can be fully established. Another factor is how easily the biometric system can be operated. Implementing a new system can be facilitated if the process of collecting and verifying biometric data is simple, such as touching a fingerprint scanner. However, implementation can be difficult if the data collection and verification processes are complex, such as what might be encountered when using multiple biometric modalities for identification. Finally, both the initial costs (due to hardware and software) and long-term costs (due to ongoing administrative and maintenance requirements) of the biometric system should be considered because they can be substantial.

While there is no one best biometric modality, some are used more often in certain settings than in others. For example, fingerprints are typically used in law enforcement, government, and human services settings, while iris, hand geometry, and palm vein are used in health care settings.[1] Each modality performs recognition (i.e., authentication and/or identification) using different physical traits. For instance, fingerprints use the physical structure of finger ridges, iris uses the colored portion of the eyes, hand geometry uses the physical structure of the hands, and palm vein uses the structure of subcutaneous veins. Each modality also has certain advantages and disadvantages that should be considered prior to implementation (see Appendix 2). For example, a proven track record is an advantage of fingerprint biometrics, while negative public perception (due to its use by law enforcement agencies) is a disadvantage. Limited physical contact with biometric sensors is an advantage of iris imaging, while lengthy staff training is a disadvantage. An advantage of hand geometry is the stability of hand patterns over time, while a disadvantage is the amount of storage space required to

[1] The discussion in this report focuses on fingerprint, iris, hand geometry, and palm vein biometric modalities because they are used in health and human services settings.

maintain the data electronically. An advantage of palm vein imaging is ease of use, while a disadvantage is physical contact with biometric sensors that may spread disease.

Use of Biometric Identification Systems in Health Care Settings

As part of this report, DMAS staff reviewed numerous documents to gain insight into how biometrics are used in health care settings. The review found that biometrics are increasingly being used due to concerns about patient safety, identity theft, and insurance fraud. Addressing these concerns is likely to become critical as the health care industry shifts toward the use of electronic medical records (EMRs) and other health information technologies as required under both the American Recovery and Reinvestment Act (ARRA) of 2009 and the Patient Protection and Affordable Care Act (PPACA) of 2010. While this shift may improve efficiency and quality of care, the potential for patient harm due to duplicate or erroneous medical records, data filing errors, benefit fraud, and identity theft may also increase. Moreover, federal legislation requires the health care industry to ensure that only authorized medical staff have access to patient records. As a result, the use of biometrics will probably increase because it offers a solution to these issues by ensuring the confidentiality of patient data and financial transactions, preventing fraud and abuse by identifying patients at health care facilities, and controlling access to secure medical data.

The document review also revealed several examples of how biometrics are used in health care settings. For example, a hospital system in Kentucky uses fingerprint traits for patient identification. Patients entering the system are required to place a finger on a scanner and the resulting samples are stored and used on future visits to positively identify patients before retrieving their medical records. A health clinic system in New York City serving both uninsured and Medicaid patients uses photographs and iris traits for patient identification and medical records management. This technology, which is 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. In addition, hospital systems in California and Florida use palm vein biometrics for patient identification and records management. Once biometric data are collected from patients, they no longer are required to show their identification and insurance cards during registration; instead, they simply place their palms over sensors located in hospital reception areas for immediate identification and registration. These hospital systems also use biometrics in emergency departments to identify patients who are either unconscious or delirious.[2] Finally, 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.

[2] Patients must first enroll in the hospital biometric systems before they can be identified in the emergency departments using their biometric traits.

Biometric Identification Systems Used by State Health and Human Service Agencies

As part of this report, DMAS staff identified four states (California, Connecticut, New York, and Texas) that use biometric identification in public entitlement programs (i.e., public assistance and/or Medicaid) primarily to reduce recipient identity fraud. Reviewing the state systems allowed DMAS staff to identify seven key points relevant to the development of biometric identification systems in public assistance programs:

1. biometrics can be implemented successfully in public health and human service programs, but exemptions may be required for certain recipient and provider groups;

2. most recipients hold positive views about biometrics and continue to participate in public assistance programs even after these systems are implemented;

3. biometric systems are expensive to operate and may not generate adequate savings through fraud deterrence unless implemented as mandatory statewide programs;

4. biometric systems must connect to other state public assistance databases to determine recipient eligibility status;

5. biometric traits can be stored as encrypted data in central databases or on special recipient identification cards;

6. biometric identification systems are implemented in public assistance programs using large databases composed of stored biometric traits from millions of individuals; and

7. collecting biometric samples from Medicaid recipients may be difficult if they are not required to perform in-person interviews to qualify for Medicaid coverage.

Additional information on the four states' biometric identification systems is presented in Appendix 3.

Virginia Medicaid Biometric Pilot Program Implementation Overview

This section provides an overview of the process that DMAS would use to implement the Virginia Medicaid Biometric Identification Pilot. Due to the complexity of developing and implementing biometric identification systems in public assistance programs, the discussion simply provides information on how the pilot could be implemented to meet the requirements of HB 1378. It should be noted that most of the topics discussed in this section would not be finalized until the agency receives federal funding to implement the pilot. The sections that follow contain information on the objectives of the pilot, recipient and provider enrollment and implementation localities, the biometric modality, system components, potential implementation scenario, the

procedures that DMAS would perform to implement the pilot, and a discussion of the pilot's associated cost savings.

Objectives. Determining the objectives of the pilot is important because they can influence the program's design and implementation. As stated in HB 1378, the objectives of the pilot are to improve efficiency and quality of care, while reducing waste, fraud, and abuse in the Virginia Medicaid program. Information collected for this report indicates that biometrics can improve efficiency and quality of care for patients in health care settings, while reducing fraud (although the extent to which biometrics has actually reduced fraud in public programs is unclear).

Biometric systems can improve efficiency by shortening the registration process for recipients at provider offices through automatic identification and insurance eligibility verification. This can reduce both waiting times for recipients and work requirements for provider staff by streamlining patient access and flow. Biometric systems also have the potential to improve quality of care by linking specific patients to their EMRs, which may reduce medical errors due to incorrect or incomplete patient records. Finally, biometric systems can reduce fraud by verifying the identity of recipients at service delivery points and by preventing providers from submitting phantom claims (i.e., claims for services never rendered) by collecting date, time, and location stamps at the point of contact.

Based on this information, it appears reasonable for DMAS to set efficiency, quality of care, and fraud reduction objectives for the Virginia Medicaid Biometric Identification Pilot. It should be possible to achieve the efficiency and fraud reduction objectives (at least to some extent) because they can be realized in a variety of provider settings. However, achieving the quality of care objective may be problematic, especially in the short-term, because many Virginia Medicaid providers do not use EMRs. This will likely change during the next several years because national health care reform legislation promotes the use of EMRs, and the Virginia Health Reform Initiative Advisory Council, DMAS, the Virginia Department of Health, and other stakeholders are working to facilitate their adoption by providers. Therefore, efficiency and fraud reduction should be viewed as short-term objectives of the pilot, while enhanced quality of care should be viewed as a long-term objective.

Recipient and Provider Enrollment and Implementation Localities. HB 1378 states that the pilot is to be implemented as a mandatory program for all Medicaid recipients residing in one urban, one suburban, and one rural locality. To verify the appropriateness of this directive, DMAS staff submitted the legislation to the Centers for Medicare and Medicaid Services (CMS) for review. According to CMS, DMAS can implement the pilot as long as participation is not a condition of Medicaid eligibility. (Therefore, the pilot program cannot be mandatory.) Because mandatory participation would represent a maintenance of effort violation under both the ARRA of 2009 and the PPACA of 2010, Virginia could lose all federal Medicaid funding if recipients were

required to participate. As a result, DMAS would implement the pilot as a voluntary program.[3]

Because the biometric pilot would be implemented as a voluntary program, DMAS would have to promote the benefits of biometrics to recipients and providers in the pilot localities. Failing to promote the pilot may result in limited participation. To promote the pilot, DMAS could develop marketing materials for distribution to recipients and providers via the agency's website, local health events, public announcements, and mailings. A central message disseminated through these efforts would be that participation is cost-free for recipients and providers because DMAS would pay for all expenses associated with the pilot. As part of its marketing efforts, DMAS could establish computer stations at community events and provider offices to demonstrate how biometric data can be captured and used for recipient identity and Medicaid eligibility verification. To facilitate recruitment and implementation of the pilot, the agency could partner with selected hospital systems and MCOs to promote the program and it may exempt certain groups of recipients (such as the elderly and disabled) and providers (such as nursing homes and pharmacies) from participation.

The pilot could be implemented in localities based on their geographic proximity. For example, the pilot could be located in and around either the City of Charlottesville or Roanoke because these areas contain all three locality types (urban, suburban, and rural). This could simplify oversight and administrative activities because the pilot would be located in one central area and it may even facilitate implementation because DMAS could partner with hospital systems and MCOs in either region to promote the program to their respective recipients and providers. Once federal funding is received to implement the biometric pilot, DMAS will work with stakeholders to identify appropriate localities for the pilot.

Biometric Modality. A variety of biometric identification modalities exist that could be used in the Virginia Medicaid Biometric Identification Pilot. Because DMAS staff lack expertise in biometrics, the actual modality that would be used in the pilot is not identified in this report. Instead, the biometric modality would be determined through a competitive request for proposals (RFP) process to ensure that the most appropriate, efficient, and cost-effective modality and operating system are selected for the pilot.

Biometric System Components. While the biometric modality is not identified in this report, certain requirements that must be met by the biometric operating system are

[3] The PPACA provides that as a condition of receiving federal financial participation under Title XIX of the Social Security Act, "a State shall not have in effect eligibility standards, methodologies, or procedures under the State plan…or under any waiver of such plan…that are more restrictive than the eligibility standards, methodologies, or procedures, respectively, under the plan or waiver that are in effect" on the date of this legislation, which is March 23, 2010. The PPACA's maintenance of effort requirement is nearly identical to the maintenance of eligibility requirement included in the ARRA, except that restrictions are measured against standards in place as of March 23, 2010, instead of July 1, 2008, and the penalty for having a more restrictive standard is more severe because it forfeits all federal Medicaid funding, rather than the increase in federal medical assistance payments provided through the ARRA.

discussed (see Appendix 4). In particular, the biometric operating system must comply with performance standards established by the federal government and other international organizations. Complying with these standards is important because they govern how biometric systems must be structured to ensure interoperability with other data exchange formats and systems. The biometric system must also include five integrated components: a sensor, signal processing algorithm, data storage, matching algorithm, and decision process. In addition, the system must be capable of performing four basic processes: collection, extraction, comparison, and decision making. Finally, the system must be subjected to several evaluations to verify its overall accuracy prior to implementation. Requiring the biometric system to comply with these elements will ensure that it is capable of correctly enrolling thousands of individuals by capturing and storing their unique biometric traits in a secure central database and rapidly (within a few seconds) and accurately identifying people and confirming their Medicaid eligibility. Contractors responding to the RFP would be required to discuss how their biometric systems will comply with these requirements.

Biometric Implementation Scenario. To illustrate how the biometric identification system could operate, DMAS staff developed an implementation scenario. To simplify implementation, recipients would not receive new Medicaid identification (ID) cards containing their biometric traits and they would not be restricted to only receiving medical services from providers participating in the pilot. Because DMAS does not require individuals to apply in-person for Medicaid coverage, provider staff would be responsible for collecting biometric data from recipients using equipment provided by the agency. A similar process was used by Texas Medicaid to implement a pilot biometric identification system in six counties. Adopting this (or a comparable) implementation scenario would ensure that the pilot complies with the requirements of HB 1378. The scenario is as follows:

> *Medicaid recipients interested in participating in the biometric pilot would be enrolled during the registration process at provider offices. Provider staff would collect recipient biometric traits (i.e., fingerprints, iris patterns, or palm vein structures) using equipment and software provided by DMAS. After data are collected, they would be converted into numeric template ID numbers and stored in a secure central biometric database. Converting the biometric traits into numeric templates would protect recipient privacy and identity because the templates cannot be converted back into actual biometric images if the database is ever compromised. As part of this process, provider staff would verify the recipients' Medicaid eligibility status through an electronic interface with the Virginia Medicaid Management Information System (VaMMIS). To the extent possible, the biometric ID numbers would be linked to recipient electronic medical records (if used by participating providers). On future visits to provider offices, the recipients would register using their biometric traits in lieu of patient sign-in sheets. The recipients' biometric traits would be matched (using one-to-one matching) to the numeric templates stored in the database for automatic identity and Medicaid*

eligibility verification. For each patient encounter, the biometric system would generate a claim entry that includes six key pieces of information: recipient Medicaid ID number, biometric template ID number, provider ID number, and the date, time, and location of the encounter. The claim entry would be stored in the central biometric database. Prior to adjudication of Medicaid claims, DMAS would receive documentation from the biometric database to verify that providers billed for services that were actually rendered (for participating recipients).

DMAS Implementation Procedures. There are six procedures that DMAS staff would perform to develop and implement the pilot. These procedures can be grouped into the following areas: authority, impact, workflow, information systems, budgeting, and RFP (see Appendix 5). To facilitate the development and implementation of the pilot, staff would perform most of the procedures concurrently rather than sequentially.

The authority procedure involves obtaining official authorization to implement the biometric pilot. This process began when the General Assembly authorized DMAS to implement the pilot through HB 1378. Because implementation is contingent on receiving federal funding, the agency may not be required to obtain additional authority (i.e., state regulations, state plan amendments, or waiver authority) to implement the pilot. However, DMAS would have to ensure that all activities involved with the development and implementation of the pilot comply with federal regulations and funding requirements.

The impact procedure involves establishing a workgroup composed of staff from DMAS and other stakeholders, such as providers, contractors, managed care organizations, and state agencies, to determine which specific groups of recipients and organizations would be affected by the pilot and what strategies should be adopted to lessen the impact of any adverse changes identified.

The workgroup would consider how implementing the pilot may affect workflow at DMAS and other organizations involved in the program. Based on the requirements of HB 1378, it is anticipated that the pilot would primarily affect DMAS. For example, HB 1378 directs DMAS to ensure that participating providers receive all equipment (including both hardware and software) and training needed to participate in the program. The legislation further directs DMAS to ensure that providers have access to continuous administrative and maintenance support (including the replacement of any equipment that becomes inoperable during the pilot), that all participants are informed of the purposes and requirements of the pilot through various outreach mechanisms, and that a process is established where participants can contact the agency for assistance concerning the pilot. The agency would develop operating policies and procedures to address these requirements.

The workgroup would also determine how the biometric pilot may affect information systems at DMAS and at other organizations. For instance, DMAS would ensure that providers have access to both the biometric database and VaMMIS for

recipient identity and eligibility verification and that biometric ID entries can be matched to actual Medicaid claims for service delivery verification prior to adjudication. This may require revising VaMMIS to accommodate provider interfaces and ensuring that a process is developed for linking biometric ID entries to provider Medicaid claims. Finally, DMAS would update its strategic plan to ensure that the biometric pilot fits within the parameters of its Medicaid Information Technology Architecture (MITA) and Health Information Technology (HIT) initiatives.[4]

The budgeting procedure involves the development of a budget based on the total amount of federal funds received to implement the pilot. The budget would identify specific activities related to the pilot's development and implementation and their anticipated costs. This document would serve as a guide to ensure that the pilot's required activities do not exceed federal funding limits.

Finally, the RFP procedure would involve establishing a separate workgroup composed of DMAS staff to develop the RFP document that would be used to solicit proposals for administering the pilot from private biometric contractors. The workgroup would also be responsible for evaluating proposals submitted by the contractors. Due to state requirements governing RFPs, this process could take up to 12 months to complete, with an additional six months required upfront to plan for the pilot program (for a total of 18 months needed to implement the pilot program upon notification of federal funding).

Cost Savings. HB 1378 directs DMAS staff to estimate the pilot's cost saving as part of the implementation report. However, staff are unable to provide an estimate at this time because several factors related to the pilot's costs and savings are unknown. For example, it is not known how much money the agency would receive to implement the pilot or which specific biometric modality and operating system would be selected through the RFP process. Moreover, the localities where the pilot would be implemented are unknown as are the number of recipients and providers likely to participate. Finally, estimating the savings that would be generated through fraud reduction and prevention is difficult (if not impossible) because the pilot would be implemented as a voluntary program. Thus, participation would probably be limited to those individuals who are least likely to commit fraud. As a result, any savings generated through the pilot would probably be marginal at best.

While DMAS staff are unable to provide a cost savings estimate, staff can provide general estimates for some costs associated with the pilot. These estimates are for illustration purposes only and no inferences should be made from them to the actual cost

[4] MITA is a federal strategy for transforming state Medicaid management information systems into state-wide, recipient-oriented systems. MITA assists states with aligning their information technology activities to their evolving business needs by standardizing interoperability, adaptability, and data exchange across organizational boundaries using nationally accepted standards. HIT provides a framework for the comprehensive management of health information and its secure exchange between recipients, providers, government organizations, and insurers. The HIT initiative encourages providers to implement EMR technology.

of the pilot.[5] Information obtained for this report suggests that the unit cost of biometric hardware typically used in health care settings varies from approximately $100 for a fingerprint scanner to almost $500 for a palm vein scanner. In addition to hardware, software used to process biometric data would need to be purchased. Staff from one vendor reported that their company leased software on a "per member per month" (PMPM) basis. Staff indicated that the PMPM cost could be as little as $0.25 per recipient. Thus, if 200,000 recipients participated in the pilot, then the monthly cost for the software would be $50,000. Staff from another vendor reported that the cost of biometric hardware and software could depend on the volume needed for a program and the extent to which the client already owned equipment that could be used to collect and process biometric data. Finally, the operation of biometric systems can represent substantial expenses for states, with overall annual costs in the millions of dollars. While not directly comparable to Virginia's planned biometric pilot, information from New York and California revealed that these states' biometric systems generated annual costs of approximately $5 million and $11 million, respectively (see Appendix 3). However, it is unclear whether the biometric programs actually generated enough savings through fraud prevention to justify their operational costs. (In fact, New York eliminated its Medicaid biometric identification program in 2008 due partly to limited evidence that the program actually reduced Medicaid fraud.)

Virginia Health Exchange Network's Eligibility and Benefits Initiative

In 2007, the Virginia Association of Health Plans, the Virginia Hospital and Health Care Association, and the Governor's Office of Health Information Technology created the Virginia Health Exchange Network (VHEN) as a collaboration of Virginia health plans and health systems. VHEN was charged with developing strategies to reduce administrative health care costs and improve service quality. One strategy developed by VHEN is an eligibility and benefits verification portal that promotes real-time information exchange between providers, health insurers, and credit card companies using magnetic swipe card technology. As part of the strategy, providers are currently being supplied with free card swipe machines that interface with Virginia health plans' eligibility databases and credit card companies' customer databases. During patient registration, provider staff swipe recipients' insurance cards through the machines to verify their insurance eligibility and to calculate and collect service copayments. While the contractor implementing the benefits and eligibility portal strategy informed DMAS staff that it is compatible with biometric technology, some providers may view the portal strategy and biometric pilot as duplicative. Implementing the biometric pilot could be difficult if many providers decline to participate because they already have access to free card swipe technology through VHEN's eligibility and benefits initiative.

[5] Staff from some vendors interviewed for this report indicated that, if given the opportunity to perform the pilot for Virginia Medicaid, they could potentially provide the biometric system at reduced costs. In fact, staff from one vendor suggested that their company could provide the system cost-free.

Summary

This report was prepared in response to HB 1378 that directs DMAS to develop a plan for implementing a mandatory biometric identification pilot for recipients in three localities. Implementation of the pilot is contingent upon receiving federal funding. Once funding is received, DMAS plans to implement the pilot through an RFP process.

Biometrics is the process of identifying specific people based on certain unique physical and/or behavioral characteristics such as face, fingerprint, signature, and walking patterns. Biometrics are used to identify individuals in many diverse settings including hospitals, airports, government facilities, and public assistance programs. In the coming years, biometrics will increasingly be used in health care settings due to concerns about patient safety, identity theft, and insurance fraud.

Information obtained for this report indicates that biometric identification systems can be successfully implemented in public health and human services programs. However, the process of implementing these programs can be complex and their operational and maintenance costs may be high. Moreover, limited evidence exists indicating how effective these programs are at achieving savings through fraud prevention, especially when implemented as voluntary pilot programs. While DMAS can implement a biometric pilot, two caveats exist that would hinder its ability to implement the program as stipulated in HB 1378. The first caveat involves the mandatory participation requirement. The pilot would have to be implemented as a voluntary program because mandatory participation would represent a maintenance of effort violation under both national economic stimulus and health care reform legislation. The second caveat concerns a free provider eligibility and benefits portal initiative that is being implemented by the Virginia Health Exchange Network. Because this initiative accomplishes goals similar to the ones that would be achieved through the biometric pilot, implementing the pilot may be difficult if many providers decline to participate.

Appendix 1

VIRGINIA ACTS OF ASSEMBLY -- 2010 SESSION
CHAPTER 870

An Act to require the Department of Medical Assistance Services to develop a pilot program for the use of biometric data to improve quality of care and efficiency and reduce waste, fraud, and abuse in the Commonwealth's Medicaid program. Approved April 21, 2010 [H 1378]

Be it enacted by the General Assembly of Virginia:

1. *§ 1. That the Department of Medical Assistance Services (Department) shall design and develop a plan for a pilot program to (i) increase the quality of care provided to recipients of medical assistance services; (ii) improve the accuracy and efficiency in billing for medical assistance services by providers; (iii) reduce the potential for identity theft and the unlawful use of recipients' identifying information; and (iv) reduce waste, fraud, and abuse in the state's Medicaid program.*

§ 2. The design of such pilot program shall include (i) implementation of a system that utilizes biometric data such as fingerprints to immediately verify a recipient's identity and eligibility for services and to create, store, and use electronic records that contain information about the type, nature, and duration of services rendered to a recipient by a provider; (ii) participation by all medical assistance services recipients in at least one urban, one suburban, and one rural county of the Commonwealth, to ensure participation of a sufficient number of persons to allow for collection of meaningful data and information; (iii) distribution of necessary equipment, including biometric readers and any cards or other materials or documents, to recipients and providers at no cost by the Department; and (iv) regular monitoring and review of individual service recipients' electronic records by the Department to identify and address inaccurate charges and instances of waste, fraud, or abuse.

§ 3. The design of such pilot program shall also include provisions (i) to ensure that all devices and systems utilized as part of the pilot program comply with standards for biometric data developed by the American National Standards Institute/National Institute of Standards and Technology and all state and federal requirements relating to interoperability and information security, including all requirements of the Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d et seq.); (ii) to ensure that service recipients' personal identifying, health, and other information is protected from unauthorized disclosure; (iii) for the development of procedures and guidelines for the use of biometric readers and other equipment to verify a recipient's identity and eligibility for services; (iv) to ensure that every medical assistance services provider and recipient participating in the pilot program is informed as to the purpose of the program, the processes for capturing, enrolling, and verifying biometric data, the manner in which biometric data will be used, and steps that will be taken to protect personal identifying, health, and other information from unauthorized disclosure; (v) to allow for actual demonstration of the data capture and verification processes for every medical assistance services provider and recipient participating in the pilot program; (vi) for addressing problems related to the loss, theft, or malfunction of or damage to equipment and any identifying documents or materials provided by the Department; and (vii) for development of a hotline or other means by which providers and recipients may contact the Department for assistance.

§ 4. The Department shall report to the General Assembly on the design and development of the plan for the pilot program, costs of the pilot program, savings associated with the pilot program, and any other pertinent information no later than 90 days after federal funding for the plan has been received.

2. That the plan for the pilot program developed pursuant to the provisions of this act shall be implemented and carried out by the Department of Medical Assistance Services upon funding for the same being provided under a federal appropriations law.

Appendix 2

Fingerprint Modality	
Advantages	**Disadvantages**
• Subjects have multiple fingers • Easy to use with limited training • Some systems require little storage space • Large amount of existing data to allow background and/or watchlist checks • Has proven effective in many large scale systems over years of use • Fingerprints are unique to each individual and the ridge arrangement remains permanent during one's lifetime	• Public Perceptions including privacy concerns of criminal implications and health concerns with touching sensors used by many individuals • Collection of high quality nail-to-nail traits requires training and skill, but current flat reader technology is very robust • An individual's age and occupation may cause difficulty in capturing a complete and accurate fingerprint image
Iris Modality	
Advantages	**Disadvantages**
• No contact required • Protected internal organ that is less prone to injury • Believed to be highly stable over lifetime	• Difficult to capture for some individuals • Easily obscured by eyelashes, eyelids, lens and reflections from the cornea • Public myths and fears related to "scanning" the eye with a light source • Acquisition of an iris image requires more training and attentiveness than most biometrics • Lack of existing data deters ability to use for background or watchlist checks • Cannot be verified by a human
Hand Geometry Modality	
Advantages	**Disadvantages**
• Easy to Capture • May be a highly stable pattern over the adult lifespan	• Use requires some training • Not sufficiently distinctive for identification over large databases • Biometric system requires a large amount of physical space
Palm Vein Modality	
Advantages	**Disadvantages**
• Non-harmful, near infrared lighting is employed • Fast, easy-to-use, and discreet • Very low false rejection rate • Compact reference pattern • Not easily replicated	• Viewed as invasive by some individuals • Depending upon the technology, may require physical contact with a sensor that must be sterilized after every use • Cost to install and maintain system can be high • Has not been evaluated by the federal government
Source: *Biometrics "Foundations Documents"*. Available from http://www.biometrics.gov/Documents/biofoundationdocs.pdf. Accessed June 20, 2010.	

Appendix 3

As part of this report, DMAS staff identified four states (California, Connecticut, New York, and Texas) that use (or used) biometric identification in public entitlement programs (i.e., public assistance and/or Medicaid) primarily to reduce recipient identity fraud. Information on the state programs is provided below.

California. In 1992, California implemented a pilot fingerprint imaging system for public assistance applicants and recipients in the Los Angeles and San Francisco areas to reduce fraud by individuals obtaining benefits under multiple identities. The program was officially implemented in 1999 as the Statewide Fingerprint Imaging System (SFIS). In 2003, the California State Auditor reviewed the program and raised several issues about its effectiveness. In particular, the Auditor reported that the state was unable to determine how effective the program was at deterring recipient identity fraud because it failed to determine the extent to which this type of fraud was occurring prior to implementing the SFIS. The Auditor further reported that due to this oversight, the state was unable to determine if the SFIS was generating enough savings through fraud deterrence to offset the $11 million it cost to operate the program annually.

Currently, all California public assistance applicants and recipients are required to be fingerprint imaged as a condition of eligibility, with the exception of dependent children and persons who are physically unable to submit biometric samples (or traits). Individuals submit fingerprint biometric traits at one of the state's local social service facilities. Each facility contains workstations consisting of scanning equipment and personal computers that capture fingerprint traits. Traits for new applicants are compared against approximately five million traits contained in the SFIS database to ensure that they have not already enrolled using false identities, while traits for current recipients are compared against existing traits to verify their identity and eligibility status prior to receiving benefits. The SFIS database interfaces with other public assistance databases and processes fingerprint traits from about 120,000 individuals monthly. To determine if the biometric requirement deterred recipients from obtaining needed services, California surveyed 550,000 recipients in the Los Angeles County area in 1995. Based on the results, the state concluded that most recipients held either positive or ambivalent attitudes toward the requirement.

In 2009, the California legislature directed the state to implement mandatory biometric sampling in its Medicaid In-Home Support Services (IHSS) program by April 1, 2010. The state complied with this directive by implementing biometric identification for this population through its SFIS. Medicaid IHSS applicants are now required to be fingerprint imaged during the application process, while recipients are imaged during the recertification process. Children, seniors, and individuals who cannot submit biometric traits are exempt. Approximately 2,400 social workers are responsible for collecting biometric traits from individuals participating in the IHSS program. Because there are over 400,000 IHSS recipients, California Medicaid staff estimate that it will take at least three years to fully implement the biometric requirement at a cost of approximately $18 million.

Connecticut. Due to concerns about fraud, Connecticut implemented a mandatory statewide biometric system in 1996. All public assistance applicants and recipients are currently required to submit photograph, fingerprint, and signature traits as a condition of eligibility. The traits are stored in a computer database and compared against existing traits to ensure that applicants have not enrolled previously using different identities and to verify the identities and eligibility status of active recipients at benefit delivery points. Biometric traits are collected at the state's 15 regional social service offices using fingerprint scanners, cameras, and digital tablets connected to personal computers linked to a statewide network specifically developed for the program. All recipients are issued new photograph identification cards after their biometrics are collected and reviewed. Biometric traits from roughly 2,000 individuals are processed monthly through the system, which costs the state about $600,000 to operate annually. Shortly after implementation, Connecticut surveyed recipients to determine their views toward the requirement. Based on the results, the state concluded that most recipients viewed the requirement positively.

According to Connecticut staff, the biometric system saved the state approximately $9 million during its initial years of operation by preventing recipient identity fraud.[6] However, staff indicated that the system may be terminated because the majority of Connecticut's public assistance recipients were transferred to Medicaid in June 2010 as required by national health reform legislation. Because Medicaid does not require biometric imaging, it may no longer be cost effective for the state to operate the system.

New York. Prior to 1995, New York operated a voluntary pilot fingerprint imaging system for adult public assistance applicants and recipients in 12 counties. Participation became mandatory in 1995 for all public assistance beneficiaries. Individuals in New York are required to submit photograph, fingerprint, and signature traits at local social service facilities before they can receive public assistance benefits. Once the traits are collected, recipients receive identification cards containing their biometric data. Traits for new applicants are compared against approximately two million traits contained in a biometric database that interfaces with other public assistance databases to ensure that they have not previously enrolled, while traits for current recipients are compared against existing traits for identity and eligibility verification. The biometric system processes traits from approximately 30,000 public assistance applicants and recipients monthly. The system costs the state about $5 million to operate annually. Based on a survey performed by New York, most recipients hold positive views about the system.

According to New York staff, the system saved the state $297 million during its first two years of operation by eliminating more than 38,000 public assistance recipients who failed to submit biometric samples. While this suggests that the system was

[6] States usually base fraud savings determinations on "cost avoidance" when applicants or recipients decline to participate because they do not wish to submit biometric traits. However, simply because an individual declines to participate does not imply that they were attempting to commit identity fraud.

successful at reducing beneficiary identity fraud, the state reinstated most of these individuals after discovering that they had failed to submit samples because they were either unaware of the requirement, did not understand it, or were unable to meet the compliance deadline.

In 2000, New York began requiring adults who qualified for Medicaid (approximately 440,000 individuals representing about 16 percent of the state's total Medicaid population) to enroll in its public assistance biometric system due to concerns about identity fraud. Recipients residing in nursing homes, receiving home health care services, or applying for Medicaid in hospitals and clinics were excluded from this requirement. Some observers questioned the feasibility of the biometric requirement due to limited evidence indicating that recipient fraud was widespread; however, the state argued that it would save money by preventing people from using false identities to obtain health care services. Nevertheless, New York eventually terminated this requirement in 2008 for two reasons: 1) it was becoming increasingly difficult to obtain biometric traits from Medicaid recipients because the state no longer required them to apply in-person for Medicaid coverage and 2) only limited evidence existed indicating that the requirement actually reduced Medicaid fraud. In fact, New York staff reported that most Medicaid fraud occurs due to providers billing the state for "phantom" services that were never rendered.

Texas. Due to concerns about recipient fraud in its public assistance program, Texas implemented a pilot biometric program known as the Lone Star Image System (LSIS) for adults in the San Antonio metropolitan area in 1996. Because of its success, the program was implemented statewide in 1999. Individuals physically unable to submit biometric samples and elderly and disabled individuals are exempt. The LSIS is structured similarly to other state biometric programs. For example, public assistance applicants and recipients are required to submit photograph and fingerprint traits as a condition of eligibility at one of the state's local social service offices. The samples are collected using workstations connected to a central biometric database that interfaces with other public assistance databases. Fingerprint traits from applicants are compared against approximately 2 million existing samples to ensure that they have not already enrolled in the public assistance program using different identities, while traits from current recipients are used for identity and eligibility verification during the recertification process and at benefit delivery points. The fingerprint traits are maintained electronically and are not included on recipient identification cards. Between 1998 and 2004, the LSIS cost Texas approximately $25 million to operate, while generating between $6 and $11 million in annual savings by preventing beneficiary identity fraud.

In 1998, Texas Medicaid implemented the Medicaid Fraud and Abuse Detection System (MFADS) as a key analytical component of the Texas Medicaid Management Information System. To support the MFADS, Texas also implemented the Medicaid Integrity Pilot (MIP) in 2004 as a front-end authentication and fraud prevention system. The Texas MIP operated for nine months and had four objectives: 1) reduce the total amount of Medicaid expenditures wasted on fraud and abuse, 2) reduce phantom billing

within Medicaid, 3) reduce fraud associated with provider up-coding (i.e., including more services on recipient claims than were actually rendered), and 4) prevent Medicaid client identification card sharing.

The Texas MIP was implemented as a voluntary program in six counties by four vendors. Approximately 228,000 Medicaid recipients and 1,215 providers (mostly hospital, physician, and dental providers) participated. Participating recipients were issued Medicaid identification smart cards. The MIP differed from the LSIS because all biometric data were stored on the smart cards instead of in a central database. To protect recipient confidentiality, the fingerprint traits were actually stored as digital minutiae maps that only represented fingerprint shapes, which made it impossible for the traits to be recreated if the smart cards were lost or stolen. Because Texas does not require individuals to apply in-person for Medicaid coverage, recipient fingerprint traits were either obtained from the LSIS (if the recipients received public assistance benefits) or were collected by providers using equipment furnished through the pilot (providers collected most of the biometric data for the pilot program).[7]

At the time of service, recipients showed their smart cards to the providers who inserted the cards into point-of-service devices that accessed encrypted data contained on the cards. The recipients then placed an index finger on a biometric scanner for identity verification based on a comparison of their actual fingerprints with the traits stored on the cards. If the fingerprints matched the traits, the recipients' Medicaid eligibility was automatically verified through an MMIS interface. Upon completion of medical services, the recipients checked-out using the same process, which generated service-visit-duration time stamps. This information was transmitted to the state for audit purposes. Texas Medicaid reported that the biometric system was widely accepted by both recipients and providers.

The Texas MIP was evaluated at the culmination of the pilot. Because the MIP operated as a voluntary pilot, the evaluation was unable to determine the extent to which it actually reduced recipient identity fraud. The evaluation was further complicated because Texas failed to determine the extent to which this type of fraud was actually occurring prior to implementing the MIP. Nevertheless, the MIP migrated into the Medicaid Access Card (MAC) program in 2006, which was a mandatory smart card/biometric identification program for Medicaid recipients and providers in three counties. While the MAC was originally scheduled for statewide implementation in 2008, it was never implemented because Texas changed the program's focus to magnetic stripe card technology.

[7] DMAS staff were unable to determine the costs of the Texas MIP. Staff in Texas did not respond to repeated attempts made by DMAS staff to interview them about the MIP.

Appendix 4

Biometric Operating System Requirements

National and International Biometric Standards: Biometric standards are developed by the National Institute of Standards and Technology and international organizations such as the International Committee for Information Technology Standards and the Organization for the Advancement of Structured Information Standards. Biometric standards are important because they specify information on technical interfaces, data exchange formats, application profile standards, and performance testing and reporting procedures. Biometric standards should be technology neutral and not favor specific vendors or modalities.

Biometric System Components: The biometric modality will be part of a system comprised of five integrated components: sensor, signal processing algorithm, data storage component, matching algorithm, and a decision process. The sensor collects biometric data and converts it into a digital format. The signal processing algorithm performs quality control activities and develops a biometric template. The data storage component maintains information for comparing new biometric templates. The matching algorithm compares new biometric templates to templates maintained in the database. Finally, the decision process involves examining the results from the matching component to make system-level decisions.

Biometric System Processes: The modality must be part of a system that follows four basic processes: collection, extraction, comparison, and decision making. Collection involves using a sensor to capture biometric traits and convert them to a digital format. Extraction takes the digital data and converts it into a compact template. In the comparison step, the biometric system measures the likeness of the template to those stored in the database. Based on the likeness, the system decides whether or not the submitted biometric matches one of the templates in the database.

Biometric Evaluations: The biometric modality and its system will be subjected to several evaluations prior to implementation. The evaluations will assess the accuracy of the signal and matching algorithms, the performance of the system in a mock environment, and its performance at the actual field sites. Performing a series of evaluations on the biometric modality and system will provide users with information on how well the system will perform when operational.

Source: *Biometrics "Foundations Documents"*. Available from http://www.biometrics.gov/Documents/biofoundationdocs.pdf. Accessed June 20, 2010.

Appendix 5

DMAS Biometric Pilot Implementation Procedures

Authority: While the General Assembly authorized DMAS to implement the pilot through HB 1378, DMAS staff will determine if any additional authority is needed by the agency to implement the biometric pilot. Examples of additional authority may include regulation, state plan amendment, federal waiver, executive order, and guidance from the Centers for Medicare and Medicaid Services.

Impact: The impact analysis procedure involves DMAS staff determining which agency divisions, state agencies, providers, advocacy groups, and contractors (i.e., health plans and others such as the agency's fiscal agent, prior authorization, and auditing contractors) will be impacted by the pilot. The procedure also involves DMAS staff determining what level of involvement and input is needed from the impacted organizations.

Workflow: In the workflow procedure, DMAS staff will determine if and how the pilot program will change workflow processes at the agency, its contractors, and providers. A team will be assembled to brain storm all possible workflow scenarios involved with the biometric pilot to determine how the program may impact various organizations and recipients. Particular emphasis will be placed on determining if the biometric pilot will change how claims are currently processed for payment by the agency.

Information Systems: The information systems procedure will involve DMAS staff determining how the biometric pilot may impact the Virginia Medicaid Management Information System as well as the agency's Medicaid Information Technology Architecture and Health Information Technology initiatives.

Budgeting: The budgeting procedure will involve DMAS staff determining how the federal funds received for the biometric pilot will be allocated among specific activities related to the development and implementation of the pilot. The budget will serve as a guide to ensure that the activities needed to implement the pilot do not exceed authorized federal funding limits.

Request for Proposals: In the request for proposals (RFP) procedure, DMAS staff will develop an RFP document used to solicit proposals for administering the pilot from private biometric contractors. Activities that DMAS staff will perform to support this procedure include developing the draft RFP document, obtaining comments on the RFP document from affected stakeholders, submitting the RFP document to review by staff at the Office of the Attorney General, and evaluating proposals submitting by vendors in response to the RFP.