TESTIMONY BEFORE THE COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON HEALTH

FOR THE HEARING ENTITLED "EXAMINING OPTIONS TO COMBAT HEALTH CARE WASTE, FRAUD, AND ABUSE"

NOVEMBER 28, 2012

BY THE

NATIONAL HEALTH LAW PROGRAM

The National Health Law Program ("NHeLP") submits this testimony to the Energy and Commerce Committee's Subcommittee on Health. NHeLP protects and advances the health rights of low-income and underserved individuals. The oldest non-profit of its kind, NHeLP advocates, educates and litigates at the federal and state levels. NHeLP's testimony addresses the use of "biometrics" for identity verification purposes in Medicaid.

Biometric technology compares an individual's physical features (e.g., fingerprint, palm, iris) to information saved in a central database to verify that individual's identity. In 2011, several state legislative proposals involved the implementation of biometric smart cards to verify the identity of Medicaid beneficiaries. Proponents for the use of biometrics in Medicaid believe this technology addresses both beneficiary fraud (by preventing card-sharing with non-enrollees), and provider fraud (by reducing phantom-billing and other forms of fraud). Yet, past experience has shown that verification programs for government benefits do not effectively reduce fraud or save money, but rather serve as a barrier to enrollment. NHeLP's testimony will:

1) demonstrate how biometric proposals create barriers to enrollment and care,
2) highlight how these proposals are a costly and misguided effort to address fraud,
3) explain the Centers for Medicare & Medicaid Services' (CMS') position on finger-imaging and other similar procedures, and
4) analyze the legality of biometric smart card proposals.

Barriers to Enrollment and Care

The stated aim of biometric programs is to reduce costs by reducing fraud. However, the evidence to date shows that identity verification programs reduce costs by discouraging eligible beneficiaries from obtaining benefits rather than by preventing fraud.

State legislative proposals in 2011 to replace existing Medicaid cards with biometric smart cards required the collection of biometric data (fingerprint, palm scan, etc.) to be stored in a central database. The proposals also required the installment of biometric fingerprint or palm scanners, as well as card readers in provider's offices, hospitals, and pharmacies, with the intent that Medicaid beneficiaries provide biometric proof of identity before receiving services and again at the completion of care or services.

If a state makes the collection of biometric data part of the Medicaid application process, this means that in addition to submitting an application, Medicaid applicants will have to go into a county social service office or other location to have this data collected. If the requirement applies to current beneficiaries as well, they would have to do the same. For some people, this additional hurdle will make it difficult to apply for Medicaid and keep those benefits. This will particularly be true for seniors and people with disabilities.

Moreover, past experience has shown that identity verification programs save money by keeping eligible beneficiaries away. In 1995, New York began requiring all public assistance beneficiaries to have their fingerprints, signature, and photograph taken at a local social service facility before the state would issue any benefits. In the first two years of the program, more than 38,000 beneficiaries lost public assistance benefits for not submitting biometric samples, saving the state $297 million.[1] Yet most of the individuals did not submit samples because they were either "unaware of the requirement, did not understand it, or were unable to meet the compliance deadline."[2] The state later reinstated benefits for most of these beneficiaries.[3]

Five years later (in 2000), New York required adults qualifying for Medicaid to enroll in its public assistance biometric system due to concerns of identity fraud.[4] However, the state terminated this requirement in 2008 because it was becoming increasingly difficult to obtain biometric data from Medicaid beneficiaries (since in-person applications were no longer required), and there was lack of evidence that the program reduced Medicaid fraud.[5] At a time when online applications are more prevalent, and the Affordable Care Act (ACA) specifically encourages states to streamline their application processes and simplify eligibility requirements to make it easier for people to get benefits, biometric smart card proposals are counter-productive and create barriers to enrollment and care.[6]

---

[1] DEP'T OF MEDICAL ASSISTANCE SERV., VIRGINIA MEDICAID BIOMETRIC PILOT IMPLEMENTATION REPORT, H. Doc. 2010-10, Reg. Sess., at A-4 (2010), *available at* http://leg2.state.va.us/dls/h&sdocs.nsf/By+Year/HD102010/$file/HD10.pdf.
[2] *Id.* at A-5.
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] ACA § 1413, 42 U.S.C. 18083.

Costly and Misguided Effort to Address Fraud

Biometric smart card proposals also are expensive to implement. In Georgia, a proposal for a statewide rollout to replace existing Medicaid cards with biometric smart cards was estimated to cost approximately $23 million for the first year.[7] Similarly, in New York a proposal to establish a "Medicaid identification and anti-fraud biometric technology program" was estimated to cost $20 million.[8] Yet, the savings under these programs are unclear, and their effectiveness questionable. Texas was one of the first states to use biometric finger-imaging in Medicaid.[9] In 2004, the state implemented the Medicaid Integrity Pilot (MIP).[10] At the conclusion of the pilot, Texas was unable to determine the extent to which the MIP reduced beneficiary fraud, in part, because it had not determined the extent to which this type of fraud occurred prior to the pilot.[11] Nevertheless, in 2006, Texas implemented the Medicaid Access Card (MAC) program, which was a mandatory smart card/biometric identification program for Medicaid beneficiaries and providers in three counties.[12] While the program was scheduled for statewide implementation in 2008, Texas dropped the fingerprint component after federal officials questioned its cost-effectiveness.[13]

Moreover, it is estimated that only ten percent of health care fraud is attributable to consumers, while eighty percent is committed by medical providers and ten percent by others, such as insurers and their employees.[14] In addition, "card-sharing" has never been proven to be a widespread problem in the Medicaid program. For example, in March 2011, during legislative hearings, the Inspector General for Georgia's Department of Community Health indicated that in the past two and a half years, there were only five reports of someone trying to use another person's Medicaid card and only three of those reports were substantiated.[15]

Those in favor of biometric technology claim it can also help stop provider fraud by reducing phantom-billing and other forms of fraud. Yet, these biometric programs place the burden on Medicaid beneficiaries to catch dishonest providers. Less costly and more effective methods of

---

[7] Letter from Russell W. Hinton, Georgia State Auditor, Dep't of Audits and Accounts, to Honorable John Albers, Georgia State Senator (Feb. 25, 2010) (on file with author).
[8] S. 4384, 199th Reg. Sess. (N.Y. 2011) (as introduced Apr. 4, 2011), *available at* http://open.nysenate.gov/legislation/bill/S4384-2011.
[9] Carrie Teegardin & Christopher Quinn, *Medicaid smart card idea raises questions*, ATLANTA JOURNAL-CONSTITUTION, Mar. 25, 2011, *available at* http://www.ajc.com/news/georgia-politics-elections/medicaid-smart-card-idea-885664.html.
[10] DEP'T OF MEDICAL ASSISTANCE SERV., *supra* note 1, at A-5.
[11] *Id.* at A-6.
[12] *Id.*
[13] Teegardin & Quinn, *supra* note 9.
[14] Sara Rosenbaum et al., George Washington University Department of Health Policy, Health Care Fraud 14 (2009), *available at* http://www.rwjf.org/files/research/50654.pdf.
[15] Teegardin & Quinn, *supra* note 9; *see also* GEORGIA COUNTY WELFARE ASSOC., REPORT ON THE 2012 SESSION OF THE GEORGIA GENERAL ASSEMB., 10 (2011) *available at* http://www.gcwa.us/documents/Reporton2011Legislation.pdf.

uncovering provider fraud exist. For example, by investing more money in Medicaid Fraud Control Units (MFCUs) rather than in biometric technology, states can obtain greater financial resources to combat fraud and can achieve greater cost savings by addressing provider fraud (the most prevalent type of fraud) .[16] The MFCU budget for an individual state is generally funded with federal grants on a 75 percent matching basis.[17] MFCUs conduct a statewide program for the investigation and prosecution of health care providers that defraud Medicaid, yet states only spend a small percentage of their Medicaid budget on their MFCUs, even though recovery amounts can be significant.[18]

CMS' position on finger-imaging and other similar procedures

In 2001, CMS (then called the Health Care Financing Administration or HCFA) clarified federal policy on the use of finger-imaging or similar procedures as part of states' Medicaid programs.[19] According to CMS, for a state to use finger-imaging procedures, it must demonstrate that these procedures will be:

- cost effective and efficient in addressing a particular identified problem,
- administered in a way that will minimize deterrents to enrollment and ongoing access to benefits for eligible individuals, and
- more effective than other procedures.[20]

CMS also requires that a state show it has explored alternatives to address the identified problem that might have less of a deterrent effect and has determined that imaging procedures are superior to those other procedures.[21]

Also, in any demonstration of cost-effectiveness and efficiency, the state must base anticipated savings on reasonable projections of savings to be achieved due to fraud detection and "not savings likely to be achieved because eligible families and individuals are deterred from applying for or retaining Medicaid coverage as a result of the procedures."[22] Finally, CMS says that states will have to demonstrate that other, less intrusive, procedures would not adequately

---

[16] While increasing MFCU resources and workforce may produce substantial cost-savings, it is important to make sure MFCUs are not denying or aggressively contesting Medicaid reimbursements for providers who perform legitimately rendered services.
[17] NATIONAL ASSOCIATION OF MEDICAID FRAUD CONTROL UNITS, MEDICAID FRAUD CONTROL UNITS, http://www.namfcu.net/about-us/about-mfcu (last visited Nov. 25, 2012).
[18] OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVICES, MFCU STATISTICAL DATA FOR FISCAL YEAR 2011, (2011), http://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/expenditures_statistics/fy2011-statistical-chart.xlsx (last visited Nov. 25, 2012).
[19] Memorandum from Cindy Mann, Director, Family and Children's Health Program to Health Care Financing Administration Associate Regional Administrators (April 4, 2001) (on file with author).
[20] *Id.*; *see also* GERALD FRALICK, NORTH CAROLINA CHIEF INFO. OFFICER, SMART CARD INITIATIVE: QUARTERLY REPORT TO THE JOINT LEGISLATIVE OVERSIGHT COMMISSION ON INFORMATION TECHNOLOGY, at 5 (Jan. 2011), *available at* https://www.scio.nc.gov/library/pdf/Smart_Cards_report_%28January_2011%29_FINAL.pdf.
[21] Mann, *supra* note 19.
[22] *Id.*

address the problem and that the state will implement the technology in a manner that is not likely to deter eligible individuals from applying for or continuing to receive benefits.[23]

Biometric proposals are likely to deter eligible individuals from applying for or continuing to receive benefits by stigmatizing Medicaid beneficiaries. Having Medicaid beneficiaries scan their fingerprint or palm every time they go in and out of a provider's office, hospital or pharmacy targets Medicaid beneficiaries by making them stand out in public settings. Only Medicaid beneficiaries will be required to do this, adding to any stigma that may already exist about receiving government benefits. As indicated in a report by Virginia's Department of Medical Assistance Services, a negative public perception exists around fingerprints because they are used by law enforcement agencies, and using fingerprints to verify the identity of Medicaid beneficiaries will intimidate people and keep them away from the Medicaid program and the health care services they need.[24]

Legality of Biometric Smart Card Proposals

To date, there appear to be no published cases where a court has ruled directly on the legality of biometric smart cards in Medicaid. However, courts have assessed state laws that impose substance abuse testing requirements for public assistance applicants and recipients. These cases provide helpful analogies to assess the validity of biometric proposals.

In *Marchwinski v. Howard*, the Sixth Circuit Court of Appeals affirmed a District Court decision holding that the suspicionless testing for substance abuse of public assistance applicants/recipients is an unconstitutional search and seizure under the Fourth Amendment of the U.S. Constitution.[25] The district court stated that "some quantum of individualized suspicion" is generally required for a search or seizure to be constitutional except in "certain limited circumstances" when "special needs" are shown.[26] The court further noted that the state had not demonstrated a special need that justified a departure from the requirement of "individualized suspicion" and failed to show that public safety was genuinely placed in jeopardy in the absence of substance abuse testing of all public assistance applicants and of random testing of public assistance recipients.[27]

Similarly, biometric data collection and verification based on a *belief* that applicants/recipients of the Medicaid program are committing fraud may also be considered an unconstitutional search and seizure. The collection of an individual's physical features (e.g., fingerprint, palm, iris)

---

[23] *Id.*
[24] DEP'T OF MEDICAL ASSISTANCE SERV., *supra* note 1, at 2-3. Other biometric options have other types of disadvantages, for example, iris imaging requires lengthy staff training, hand geometry requires a large amount of storage space to maintain data electronically, and palm vein imagining requires a certain amount of physical contact with biometric sensors, which may spread disease. *Id.*
[25] 60 Fed. App'x. 601, (6th Cir. 2003), *aff'ing* 113 F. Supp. 2d 1134 (E.D. Mich. 2000).
[26] *Id*. at 1138.
[27] *Id*. at 1139-1140.

compared to a central database each time the Medicaid beneficiary receives services is not much different from the collection and testing of a urine sample, which is considered a "search" within the meaning of the Fourth Amendment.[28] States have proposed to collect biometric data without an individualized suspicion of fraud, and simply believe "some" people in the Medicaid program are committing fraud. As in *Marchwinski*, there are no special needs showing a public safety concern that would justify a suspicionless search. Standards and methods for determining Medicaid eligibility must be consistent with rights of individuals under the U.S. Constitution and civil rights laws.[29] Therefore, if biometric data collection is a violation of the Fourth Amendment, it would be unconstitutional and could not be used as a standard for determining Medicaid eligibility.

In *Lebron v. Wilkins*, a district court granted a preliminary injunction finding that a Florida law requiring all Temporary Assistance for Needy Families (TANF) applicants to submit to suspicionless drug testing is highly likely to violate the Fourth and Fourteenth Amendments.[30] The plaintiff contended that the state's drug testing program violated his right to be free from unreasonable searches.[31]

As background to the case, in 1998, the Florida legislature enacted legislation that required the Florida Department of Children and Families to develop and implement a "Demonstration Project" to study and evaluate the impact of drug-screening and testing on TANF applicants' employability, job placement, job retention and salary levels, and make recommendations based, in part, on a cost-benefit analysis.[32] The recommendation at the end of the project was not to expand it because of the high costs of drug testing compared with the benefits derived, and the "minimal differences in employment and earnings between those who showed evidence of current substance abuse and those who did not."[33]

Yet in 2011 the Florida legislature "resurrected" the concept of drug testing TANF applicants.[34] No new studies were conducted, and no new data was offered. Nevertheless, on July 1, 2011, Florida began drug testing TANF applicants.[35] In the program's first month, preliminary results from drug testing showed that only 2% of applicants tested positive.[36] Applicants who did not take the drug test were denied benefits.[37] The district court mentions that some of these denials may be due to the statute's deterrent effects, for example: inability to pay for the drug test, lack of "approved" laboratories near the applicant's residence, inability to secure transportation to a

[28] *Marchwinski, supra* note 25.
[29] 42 C.F.R. § 435.901.
[30] 820 F. Supp. 2d 1273 (M.D. Fla. 2011).
[31] *Id.* at 1276.
[32] *Id.*
[33] *Id.* at 1278.
[34] *Id.*
[35] *Id.* at 1278,1280.
[36] *Id.* at 1280.
[37] *Id.* at 1281.

laboratory, or refusal to accede to what an applicant considers an unreasonable condition to receive benefits.[38] Ultimately, the court held the state had not shown evidence that any TANF funds would be saved by instituting the program, or that there would be any financial benefit or net savings due to the passage of the statute.[39]

In a very similar way, biometric smart card policies produce questionable cost-savings and cause the same deterrent effects. As explained more fully in the sections above, the evidence to date shows that identity verification programs reduce costs by discouraging eligible beneficiaries from obtaining benefits rather than by preventing fraud. This was the case in New York where tens of thousands of beneficiaries were removed from public assistance for not submitting biometric samples, and eventually this requirement was removed, in part, because of lack of evidence that the program reduced Medicaid fraud.[40]

Conclusion

Biometric smart card programs claim to reduce fraud and save state resources, yet they place an undue burden and stigma on Medicaid applicants and beneficiaries. Past biometric technology programs have not proven to be cost-effective and have deterred eligible beneficiaries from enrolling in the program and receiving services. The vast majority of Medicaid fraud is committed by providers, not beneficiaries, and there are other less costly ways to address provider fraud. Finally, the legality of biometric smart card proposals is questionable, and it appears the collection of biometric data in Medicaid would be considered unconstitutional.

For further information or questions about this testimony, please contact Michelle Lilienfeld at the National Health Law Program, (310) 204-6010 or lilienfeld@healthlaw.org.

[38] *Id.*
[39] *Id.* at 1290-1291.
[40] DEP'T OF MEDICAL ASSISTANCE SERV., *supra* note 1, at A-4, 5.