



Texas Medicaid

In 1998, the Texas Health and Human Services Commission (HHSC) decided to implement the Medicaid Fraud and Abuse Detection System (MFADS). The MFADS is a key analytical component of the Texas Medicaid Management Information System (MMIS). The number of cases investigated, the dollar amounts identified, and dollar amounts recovered have increased as the result of productivity and efficiency increases generated by the MFADS research tools and ad hoc query-reporting capabilities.

This increased investigative activity and HHSC's consistent enforcement of Medicaid policy and procedures have deterred fraud and abuse in the Medicaid program. At the same time, new schemes, patterns, and trends of fraudulent behavior have arisen. HHSC is continuously working to address these new challenges and continues to believe in exploring new technology to enhance the MMIS.

One of the most consistent fraud patterns involves what are sometimes called "phantom" services—where some providers appear to be billing for services that they are not actually providing. Currently, the only way to identify this type of abuse is to request medical records and confirm the services with the patients, which can be very labor intensive and costly.¹

HHSC therefore initiated the Medicaid Integrity pilot study, to design and develop a front-end authentication and fraud prevention system. The system had multiple purposes:

- Create a more efficient Medicaid system by reducing the total amount of Medicaid expenditures wasted on fraud and abuse
- Alleviate "phantom billing" within the Medicaid system
- Reduce the amount of fraud associated with provider up-coding
- Prevent client Medicaid ID card sharing and card swapping

How Medicaid Integrity Works

The Medicaid Integrity system works as follows. Clients are automatically issued new Medicaid ID smart cards. At the time of service, the client shows the ID card to the provider. The provider inserts the client's smart card into a point-of-service device to access the data encrypted on the card. The client then places a finger on a biometric scanner. Client identity is validated in less than 1 second. The client then proceeds with normal medical service.

Upon completion of the medical appointment, the client checks out, using the same process and thereby creating a service-visit-duration time stamp. This information is transmitted to the state and ultimately compared to the bill prepared by the provider and submitted to the Medicaid office for payment.

How Medicaid Integrity Helps

Table 1 summarizes how the Medicaid Integrity program supports fraud detection and deterrence.

¹ Health and Human Services Commission Request for Proposals for Front End Authentication and Fraud Prevention System Pilot Program, RFP #529-04-085, October 1, 2003.

Table 1. Fraud Detection in the Texas Medicaid Integrity Smart Card Program

Fraud Type	Description	Smart Card Benefit Achieved
Phantom billing	Claim is submitted, but no services were rendered. Client is not even physically present at provider's office.	Verifies client is physically present in the provider location at the time of service.
Up-coding	Provider's claim includes more services than were actually rendered.	Provides time-stamped visit <i>duration</i> data. This data is compared to provider billings to identify up-coding fraud.
Card-sharing and ID theft	Ineligible individual uses another's valid Medicaid ID card to receive services.	Verifies entitled client is the only one using the card.

Medicaid Integrity Pilot² Description

The Medicaid Integrity pilot study was conducted in six counties. Four vendor teams were responsible for the development, implementation, and operation of the pilot. During the pilot, information was collected to validate the client's presence at the point-of-service, including date, time, and duration of service. This information was compared with traditional Medicaid billing data received by the state.

The initial 9-month pilot involved the voluntary participation of 1,215 Medicaid providers and 228,131 Medicaid recipients and the installation of 954 front-end authentication devices. This level of participation allowed data to be collected from 60,196 client visits and 122,233 transactions. Because the program was not implemented statewide, it is not possible to clearly establish Medicaid fraud reduction from the pilot results. However, biometrics and smart cards were determined to be an effective tool in preventing provider and client fraud within the Medicaid program.

The entire Independent Evaluator Report is available at http://www.hhsc.state.tx.us/OIE/MIP/020105_MIP_EvalRpt.pdf. Further details about the program are available at the HHSC Web site, http://www.hhsc.state.tx.us/OIE/MIP/MIP_Updates.html.

This profile was developed by the Smart Card Alliance Healthcare Council for the white paper, "Smart Card Applications in the U.S. Healthcare Industry." For more information about how smart cards are used for secure identity and other applications, please visit the Alliance web site at <http://www.smartcardalliance.org>.

² *Front End Authentication and Fraud Prevention System Pilot Program Medicaid Integrity Pilot Status Report, July 1, 2005.*