Use of Open Networks for Medicaid Eligibility and Fraud Prevention

State Senator Heather Steans

Presented by Castlestone Advisors, LLC

December, 2010

- *From the confirmation testimony of Dr. Donald Berwick, nominated to become administrator of CMS, to the Senate Finance Committee, November 17, 2010:*

-- "*New tools and authorities to fight fraud: New authorities in the Affordable Care Act offer additional front-end protections to keep those who commit fraud out of Federal health care programs, as well as new tools for deterring wasteful and fiscally abusive practices, promptly identifying and addressing fraudulent payment issues, and ensuring the integrity of the Medicare and Medicaid programs. CMS is pursuing an aggressive program integrity strategy that will prevent fraudulent transactions from occurring, rather than simply tracking down fraudulent providers and pursuing fake claims. CMS also now has the flexibility needed to tailor resources and activities in previously unavailable ways, which we believe will greatly support the effectiveness of our work ..*"

Dr. Berwick is referencing Castlestone Advisors' demonstration project to prevent fraud and abuse in the Medicare Durable Medical Equipment Program

The Medicaid Landscape:

- Increasing burden on states due to health reform
  - IL forecast: 25% increase in enrollment by 2019
  - $13 Billion budget deficit

- Rapid Eligibility fluctuations
  - Changes in Eligibility baselines=changes in rolls
  - Exchanges and “connectors”
  - Changes in service provisions, co-payments, multiple payers (State, private, individual) and types of programs

- Current methods of eligibility checking , IVR and web, are time consuming for busy office practices

- Fraud *prevention* and *detection* increasingly difficult—
  - Illinois must verify visits to 70,000+ locations
  - Prompt Payment requirements in force
  - This forces fraud “reduction” to retrospective **Pay and Chase**

Fraud is all to easily perpetrated with 2.5 million beneficiaries and 70,000 locations

- ***Prompt Payment Requirements*** **mandate rapid payments after claim receipt**

- **The HFS cannot possibly monitor whether 2.2 Million beneficiaries received services in over 70,000 locations prior to payment without help**

- ***Current tools*****:**
  - **Data available= claims data**
  - **Data unavailable= verification that individual received services or set foot in a provider office- historically been to costly to certify**
- ***Current Practices*****:**
  - **"Snitch lines", report fraud**
  - **Sifting through mounds of data- however**
    - **Clinical patterns change**
    - **Data is not detailed enough**
    - **Data is often improperly coded**

Our approach= Verify, then pay

- This Requires:
  - **<u>We can verify that a beneficiary was in the office when the claim stipulates</u>**
    - The ability to attest that services were rendered when the claim stipulates
    - A data source independent from claims to verify patient presence
    - Accurate data in *<u>sufficient detail</u>* and *<u>speed</u>* to act on
    - *<u>Cost effectiveness</u>* in data collection and support
    - *<u>Complement</u>* to data-intensive pattern recognition systems

We address many of the frauds listed as problem issues

- Services not rendered:
  - *Verify time and location of beneficiary*
- Durable Medical Equipment and Prescription Drug Fraud
  - *Our current project with Medicare to verify prescriptions in real time using the card networks*
- Physician Identity Theft
  - *Claims have to have the double security of a identified card and verified swipe terminal for a claim to be accepted*

Published problem areas from the FBI and other sources:

- ***The FBI Financial Crimes Section identified the most common types of healthcare fraud as:***
  - 1) **billing for services not rendered**;
  - (2) up coding (charging a higher value for services than is appropriate);
  - (3) duplicate claims;
- ***From the National Summit on Healthcare Fraud 2/1/10***
  - *Unquestionably, many of the cases cited at the Summit fall in this category – billing for services not rendered*, *beneficiaries selling their Medicare and Medicaid numbers*, false certifications by physicians for items of durable medical equipment
- , ***National Journal 11/09***
  - "..Blue Cross states that at least 75% of health care fraud is committed by the provider and 18% by the patient. The largest type of provider fraud (approximately 36%) is billing for services not rendered."
- ***Other areas of concern to the FBI Financial Crimes Section include***
  - **durable medical equipment**,
  - hospital fraud**,**
  - **physician fraud**,
  - **home health agencies**
  - **beneficiary-sharing**,
  - chiropractic,
  - **pain management and associated drug diversion**
  - **physical therapists, prescription drugs,**
  - **identity theft which involve physician identifiers**

We can verify nearly every outpatient claim in the State of Illinois

- We create a private network for Medicaid and State Programs atop the credit card networks
- Medicaid ID cards are issued with a magnetic strip that allows the card to send information over the MasterCard rails anywhere in the world
- Card is swiped at the provider office to determine eligibility (standard ANSI 270/271 transaction)
- Transaction is *time stamped* and *location* and *recipient* are identified and available ***within 15 seconds*** to the HFS or law enforcement

Why this works today

- **Over 96% of Medical Offices can process credit card transactions already paid for by providers**
  - **Each swipe terminal is already known to the network**
  - **Highly cost effective for the State to implement**
- **Each transaction is *time stamped, location identified and independently transmitted***
  - **Location of recipient swipe cannot be manipulated**
  - **Data is available in real time and time-based transaction activity-like credit card fraud- is detectable**
- **Card swipe matched against claim prior to payment**
  - **Match on Date of Service, Recipient ID, Provider ID**

How it gets implemented

- Cards issued to recipients and providers
  - Encoded with only 16-digit number-details stored on server
  - No personal information on the Card
  - Lost/Stolen cards immediately deactivated-like credit cards
- HFS gets portal to view transactions and manage cards
  - Cancel lost or stolen card
  - Analyze Transaction Data
  - Issue card from Portal
  - View transactions by provider/time

Cards can be managed centrally by HFS

- Lost or stolen cards are instantly deactivated- attempts to use them will be tracked by time and location
- Cards are good for 3 years and can be activated or deactivated as eligibility changes no need to continue to issue cards periodically
- Single card can be used across changes in payers (exchanges) for better tracking and reconciliation (Castlestone patent)
- Additional security features (card pictures, PINs stored picture) can be added

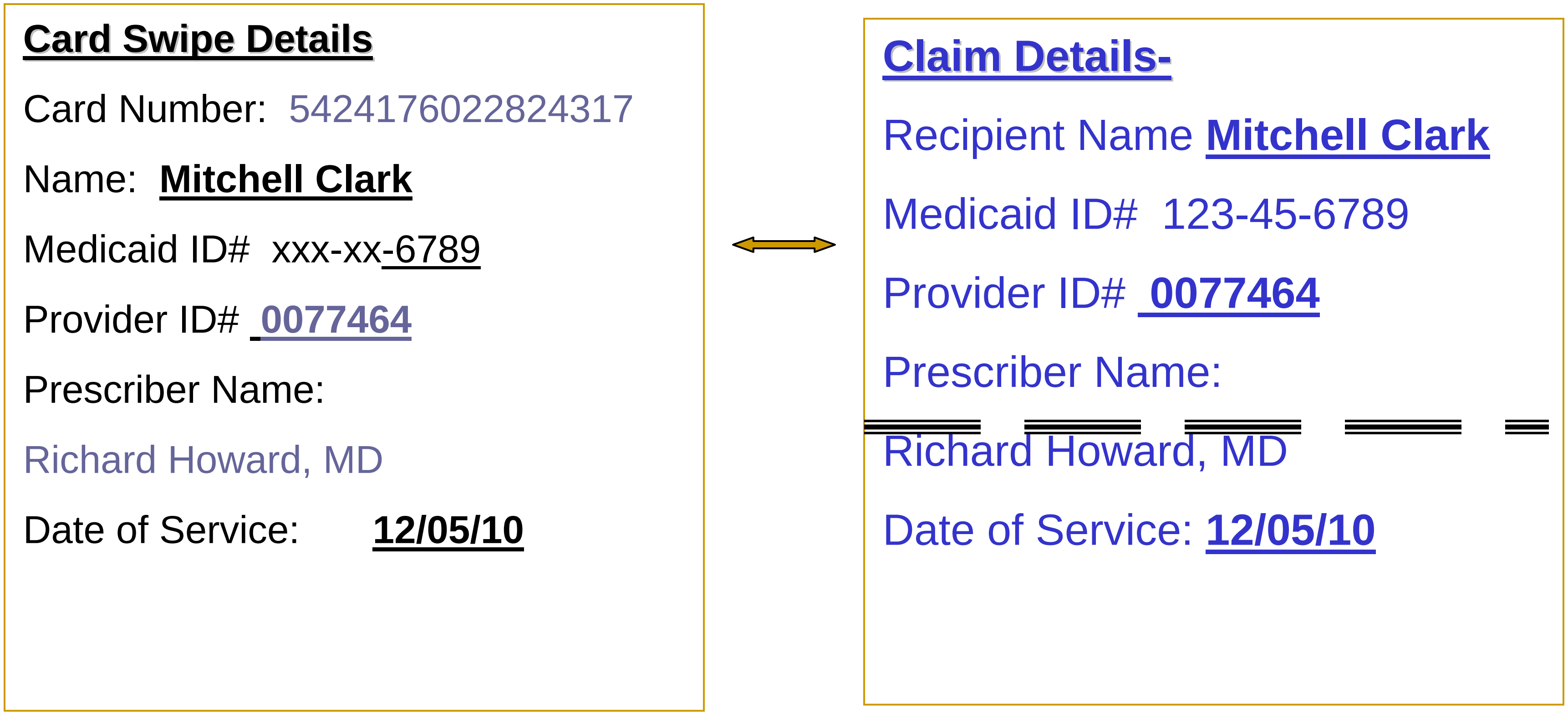
CASTLESTONE Advisors LLC

Security is better and more easily managed

- ***Eligibility requests*** using web systems can give unscrupulous providers a list of beneficiaries to claim under. *Using the card to originate the request is more secure than allowing open internet access- fewer access points to manage and secure*

- ***Access Medical Records*** for secure health information exchanges
- ***Cards are encrypted*** and only when authorized by the card networks can they transmit information
- ***No SSI, Case Number on the mag stripe*** for prevention of identity theft. Information is stored and encrypted, on the servers
- ***Reported Lost/stolen cards deactivated within 30 seconds*** across the network

When the Claim Arrives, it is Matched- ***Prior to Payment***



Card Swipe Details

Card Number: 5424176022824317

Name: **Mitchell Clark**

Medicaid ID# xxx-xx-6789

Provider ID# **0077464**

Prescriber Name:

Richard Howard, MD

Date of Service: **12/05/10**

Claim Details-

Recipient Name **Mitchell Clark**

Medicaid ID# 123-45-6789

Provider ID# **0077464**

Prescriber Name:

Richard Howard, MD

Date of Service: **12/05/10**

Where this contributes to fraud fighting efforts:

- ***Services Not Rendered*** – the most common and costly category of fraud (12% est. in Medicare) - phantom patients can nearly be eliminated
- ***Transportation , home care and adult day care Fraud***- if a patient does not appear at a physician appointment, do not pay the transportation company. Mobile swipe readers can also be used- such as our iPhone or Android swipe terminal with GPS.
- ***Real Time Alerts-*** for attempts to use cancelled cards, e.g.
- ***Dead Doctor Billing*** Dead doctors cannot swipe card in non-existent offices.
- ***Card Sharing & Odd-hour billing*** Real time information with time stamps can help detect unusual card or provider activity – complements other data mining with information otherwise not available
- ***DME and Controlled Substances Claims-*** we can verify prescriptions
- Castlestone has been awarded a contract to use its technology to prevent fraud and abuse in the Medicare Durable Medical Equipment progam, as seen on 60 Minutes and other news programs
- ***Verification of Managed Care Billing*** State Medicaid and Managed Medicaid can oversee the activities of managed care recipients better if they issue the identification card to all recipients (Castlestone patented)
- ***Beneficiary "Locks***" We can verify the location of outpatient or pharmacy claims and deny in real time attempts to use outside the specified offices or pharmacies
- ***Prompt Payment Regulations*** can pend/suspend payments if conditions not met prior to payment, as suggested by pending legislation

Cost & Implementation Considerations

- *Card Creation*: We create/activate/deactivate and manage cards based on DPW guidelines
- *Hardware cost for providers* –***NONE***. uses existing credit card terminals
- *Network Costs for DPW*: ***NONE***. We use the MasterCard network for transactions
- *Systems & Programming Costs* we can provide web access to offices to issue cards; S&P can be very simple data exchange of new/change/delete clients or full real time integration
- *At-risk success fee/Transaction Fee-* **Transaction Fees can be billed to providers to pay for entire program with State participating in the revenues. We are willing to go at-risk for a portion of our fees**

Benefits of Verifying Presence at Point of Care

- **2.500,000 Medicaid Recipients**
- **$12.5 Billion Annual Budget**
- **$4.4 Billion in outpatient claims**
- **10% of expenditures estimated to be fraudulent or abusive-GAO numbers**

- ***Capturing every outpatient encounter, we estimate:***

- **Preventing only 3% of inappropriate payments results in an 145% *ROI based on our highest estimated costs borne by the State* and does not account for cost savings from reduced recapture tasks, such as prosecution, research, CMS reimbursement**
- **ROI is even greater than post-payment recovery methods, with 65% of the funds going back to CMS- no payment due CMS for savings**

Benefits to State of Illinois

- ***Existing infrastructure*** **Will work with any industry standard card terminal- medical offices already paying for service; no need to add PMS if it does not exist**

- **Nearly all providers can participate today- 70,000+ Illinois based providers can transact *today* with this technology-more securely than other transactions- no new hardware or software required at the provider office**

- ***Meeting Changes to Prompt Payment Legislation*** **Can pend/suspend/postpone payments if swipe not present. Increased cash balances may pay for program. Other cash management methods can be tied to this**

- ***Real Time Member and Provider Eligibility*** **Card/provider access turned on/off in real time for more accurate eligibility and less subrogation**

- ***Little IT resource required to implement*** **--Encounters can be submitted using existing processing systems, infrastructure is outside MMIS, integration at 2 points**

- ***Payers are Familiar with the Technology*** **Office staff knows how to use card swipe machines, Medical Group Management Association asking payers to issue magnetic strip cards**

- ***Complementary to other fraud detection methods*** **The time and location stamps can uncover patterns of claims previously unavailable (** large claim volume on certain times, claims from multiple offices within impossible time frames for a single provider, other spikes in activity in time periods) **that are matched against other outlier patterns**

Contact

Jeff Leston

President
Castlestone Advisors LLC
(212) 874-4390
jeff.@castlestone-llc.com