Department of Health and Human Services

Centers for Medicare & Medicaid Services

Medicaid Integrity Program

Connecticut Comprehensive PI Review Final Report

November 2007

Reviewers:
Mark Rogers, Review Team Leader
Todd Chandler
Claudia Simonson
Joel Truman

Table of Contents

EXECUTIVE SUMMARY

The Centers for Medicare & Medicaid Services (CMS) is committed to partnering with States and other stakeholders to combat fraud and abuse in the Medicaid program. As part of that commitment and to provide oversight, CMS staff conducted a review of Connecticut's Medicaid program integrity policies and procedures. The review team met with various managers and staff with the Connecticut Department of Social Services (DSS) and the State's Medicaid Fraud Control Unit (MFCU).

DSS has a number of commendable practices in place to protect the integrity of the Connecticut Medicaid program. They include data mining to identify potentially inappropriate payments combined with an active provider auditing program. On average, DSS audits 174 providers and collects $8.8 million annually from provider overpayments. Additionally, DSS frequently and aggressively screens its providers to prevent excluded parties from participating.

The review team identified three Federal regulatory findings during its review. Those regulations are:

- 42 CFR § 455.21(a)(1), requiring the State to refer all cases of suspected provider fraud to the MFCU.
- 42 CFR § 1002.3(b), requiring the State to report any action it takes on a provider's application for participation in the program to the Department of Health and Human Services Office of the Inspector General (HHS-OIG).
- 42 CFR § 455.106(b)(1), requiring the State to refer provider criminal conviction information to HHS-OIG.

DSS also has a number of areas of vulnerability. It is apparent that serious communication and trust issues exist between DSS and the MFCU. This is, in large measure, why only 12 fraud referrals have been made by DSS to the MFCU in the last three years. DSS also has very few established procedures for monitoring the fraud and abuse activities of Managed Care Organizations, which is critical for the integrity of the State's managed care program. Finally, there are relatively few written program integrity policies and procedures in DSS.

The draft of this report was provided to the State Medicaid Director, the State Program Integrity (PI) Director and the Medicaid Fraud Control Unit Director. The State's responses, as reflected in this final report, are those of the PI Director. The State Medicaid Director advised he had no additional comments. The MFCU Director did not provide any comments.

The State of Connecticut took exception to two of the draft findings. Its response has been included in its entirety as Appendix A to this report. CMS stands by its conclusions. However, this final report reflects technical corrections suggested by the State. The

State's responses to the findings and areas of vulnerability are included in the body of this report along with CMS' response to those comments as appropriate.

I. INTRODUCTION

During the week of March 5-9, 2007, four staff members from the CMS Medicaid Integrity Group (MIG) conducted a comprehensive Program Integrity (PI) review of the Connecticut Medicaid Program.[1] The review team was onsite at the Connecticut Department of Social Services (DSS) offices for most of the week but also visited DSS' fiscal agent and the State's Medicaid Fraud Control Unit (MFCU). The team had four goals: a) determine Connecticut's compliance with Federal laws and regulations related to program integrity activities; b) identify other program vulnerabilities as well as noteworthy and possible benchmark practices; c) look for opportunities to provide technical assistance in the future; and d) help this State improve its overall program integrity efforts.

During the onsite visit, the team met with the Director of the Office of Quality Assurance (OQA) and his key staff, the Director of Medical Operations, the Director of Managed Care, the Director of the MFCU and key investigative and fiscal agent staff. The team also had a conference call with representatives of one Medicaid managed care contractor.

This review focused on the activities of OQA, which is primarily responsible for Medicaid program integrity. However, the Medical Operations and Managed Care Divisions also play an important part in fighting fraud and abuse in Connecticut's Medicaid program. Connecticut's SCHIP program operates under Title XXI of the Social Security Act, and was, therefore, not included in this review.

Background - The Connecticut Medicaid program is administered by DSS. As of February 2007, the program serves approximately 400,000 recipients, with 24 percent enrolled in fee-for-service (FFS) and 76 percent enrolled in four Medicaid managed care plans. DSS has enrolled 6,699 FFS providers representing 28,847 performing providers. The four managed care organizations contract with 15,247 providers.

Medicaid expenditures in Connecticut for State fiscal year ending June 30, 2006 totaled $4,122,843,001. Fifty percent of the cost of medical services is supplied by the Federal government. Expenditures for managed care enrollees account for 17 percent of the total, despite the high proportion of managed care enrollees. DSS' highest cost recipients--SSI recipients and dual eligibles, including institutionalized recipients--remain largely within the FFS program. DSS has processed an average of 16.6 million claims per year for the past three years for its FFS providers.

[1] Unless otherwise noted, financial information about program integrity activities cited in this report was provided by the DSS. DSS provided collections information for the last three State fiscal years, which run from July 1 to June 30. For purposes of this report, the review team accepted Connecticut's representations and did not independently verify any staffing or collections information provided to it.

II. SUMMARY OF REVIEW

A. Program Integrity

Federal regulations at 42 CFR Part 455 mandate that all State Medicaid programs engage in the detection, investigation, and reporting of suspected fraud and abuse. In Connecticut, the organizational component dedicated to anti-fraud and abuse activities is OQA, located within DSS.

Staffing - At present, OQA has approximately 90 full-time employees (FTEs). According to the OQA Director, approximately 65 of these employees perform functions that are not directly involved with Medicaid provider fraud. They perform third party liability collections, the auditing of non-Medicaid grants to other agencies, and the monitoring of recipient fraud. While oversight of recipient fraud is an important State program integrity function, the focus of this review is the prevention and detection of provider fraud in the Medicaid program. Approximately 25 of OQA's FTEs are dedicated to this function, chiefly through the auditing of Medicaid providers. OQA also contracts with an outside contractor, Craig J. Lubitski Consulting, LLC, for nursing home audits.

Investigations - Based on interview responses and documentation provided in the course of the review, the Connecticut Medicaid program meets the requirements of 42 CFR § 455.13 in that it has methods for identifying, investigating and reporting suspected fraud. Program Integrity staff in OQA are able to identify possible targets for review through information from a variety of referral sources. These include calls from a State-maintained toll-free fraud and abuse hotline, issues identified through data mining efforts or traditional Surveillance and Utilization Review Subsystem (SURS) data runs, and, to a lesser extent, feedback from recipients on sample Explanations of Medicaid Benefits (EOMB) issued by DSS for client review.

Once OQA receives a complaint or identifies a pattern of suspected fraud, the complaint is referred to PI staff for a preliminary investigation conducted with targeted queries using OQA's data warehouse, traditional SURS data runs, or both. In the normal course of a preliminary investigation, following a paid claims analysis that establishes the possibility of fraud, OQA will refer suspected cases to the MFCU in the Chief State's Attorney's Office.

Administrative Actions - Connecticut's program integrity operation is effective in taking administrative actions against identified problem providers and has a wide range of tools at its disposal. OQA has full subpoena power over provider records. OQA will take actions, such as recoupments and withholdings, against providers whom it believes continue to inappropriately bill the Medicaid program even while possible criminal actions are being deliberated or are on hold. If a provider is not currently billing Medicaid, a case can be referred to the State Attorney General's Office for collection action.

Providers targeted by OQA receive written notification when a suspension action is initiated against them. If they do not respond within 30 days, the administrative action proceeds without further appeal remedies. State law does not require OQA to conduct a full audit of providers for which there is evidence of an overpayment but for which there is no evidence yet of a pattern of systematic fraud or abuse. It can issue a paid claims adjustment request, which is a swift, smaller-scale recoupment action against which there is no administrative recourse. OQA will grant an administrative review and full appeal rights prior to initiating a suspension, but it has extensive freedom of action to take economic sanctions short of suspension.

OQA makes significant efforts to educate providers before resorting to aggressive administrative actions. Its senior staff regularly address the annual meetings of groups, such as behavioral health providers, pharmacists, and residential treatment facility operators, to communicate policy standards and offer guidance. If it uncovers widespread billing issues, OQA will work closely with the Medicaid section to develop provider bulletins that give notice of policy expectations before administrative actions commence.

The OQA Director reported that, in July 2005, State legislation placed some curbs on its freedom of action against problem providers. Public Act No. 05-195 states that:

> *a finding of overpayment or underpayment to a provider in a program operated or administered by the department . . . shall not be based on extrapolated projections unless (A) there is a sustained or high level of payment error involving the provider, (B) documented educational intervention has failed to correct the level of payment error, or (C) the value of the claims in aggregate exceeds one hundred fifty thousand dollars on an annual basis.*

In effect, this law has limited OQA's ability to use statistically valid claims sampling and extrapolation techniques to collect overpayments from smaller providers, although OQA's data warehouse has offset some of those concerns by conducting targeted data queries. There is also concern about the effectiveness of OQA's recoupment operations if additional legislation succeeds in further restricting the use of extrapolations.

Case Tracking - Although DSS was cited in the past by State auditors for problems in tracking reported fraud complaints, OQA was able to produce sample case tracking forms which are now used to track the status of reported complaints. The OQA auditors also track the status of overpayments found and recovery actions. In general, OQA claimed it had tightened up its procedures for tracking complaints related to fraud and abuse cases.

Provider Attestations and Recipient Verification Procedures - The Department of Social Services complies with Federal regulations at 42 CFR § 455.18 which require a provider's attestation that the information provided on claim forms is accurate. Such a statement exists on both the paper and electronic forms. In the fee-for-service Medicaid program, DSS is also compliant with regulations at 42 CFR § 455.20, requiring that States have a method for verifying that recipients received the services for which their

providers submitted claims. DSS' Medicaid Management Information System (MMIS) contractor, Electronic Data Systems (EDS), regularly generates EOMBs for a random sample of recipients who are asked to verify the receipt of services. OQA reports that there is an extremely low rate of return from recipients and that the use of EOMBs is only minimally helpful as a source of information. The MIG review team did find issues in implementing recipient verification procedures for managed care enrollees. The managed care recipient verification procedure is addressed in Section G of this report.

B. Surveillance and Utilization Review Subsystem/Other Data Systems

In the past three State fiscal years (SFY), DSS processed the following volume of claims through its MMIS:

SFY	Volume of Claims
2006	17,400,000
2005	16,800,000
2004	15,200,000

EDS is the fiscal agent responsible for claims processing and adjudication as well as for the input of claims data into and maintenance of OQA's data warehouse. Connecticut does not have a SURS unit. Instead, the SURS function is performed in OQA's Medical Provider and Contract Audit Division. According to OQA senior staff, SURS reports and analysis are no longer used as a primary tool for identifying problem providers. Rather, they are generated as backup confirmation for queries developed through OQA's data warehouse, a resource which now gives many components within the Connecticut DSS much faster access than ever before to standard and customized reports and the ability to do innovative data mining.

Data Analysis/Mining - The Connecticut Data Warehouse Business Intelligence System went online in December 2005 and became fully operational in March 2006. Two years of Medicaid claims were initially loaded into the warehouse. It currently houses five years of data. Developed by EDS and originally based on a Pennsylvania model, Connecticut's data warehouse employs a number of tools which support both simple and complex data analysis and mining efforts. The data warehouse can produce standard reports using Business Objects and DSS Profiler to build Management and Administrative Reporting (MAR), Surveillance and Utilization Review (SUR), and MAR/Detail reports. EDS is responsible for providing a specified number of standard queries. The fiscal agent contract also requires EDS to develop a smaller number of customized or ad hoc queries for OQA on request.

EDS manages the operation of and provides tools to retrieve data from the data warehouse while DSS manages it. State PI staff have direct access to the data. The OQA manager who monitors the EDS contract stated that approximately eight PI staff perform intensive data mining with the system. Queries are run for numerous components within DSS. The availability of five years of data permits much deeper longitudinal studies than were previously possible. Data runs can also be done in a much shorter time than was

possible using traditional SURS reports. As a result of data mining activities using the warehouse, PI staff have devised new edits that would be useful to incorporate in the claims processing system. However, DSS is waiting to implement them because it plans to bring up a new MMIS in October 2007. The new MMIS will also be managed by EDS, which recently won an extension of its fiscal agent contract. The new MMIS will replace the legacy system with a relational database. While waiting for these edits, PI staff are using targeted queries and standard reports residing in the data warehouse to identify claims which the edits would otherwise flag.

During the interviews, OQA noted that the MMIS and data warehouse capture and house managed care encounter data as well as FFS claims data. PI staff believe that while the encounter data is generally useful and accurate at the recipient level, there are unresolved problems in linking recipient and service level data to specific providers. While OQA has analyzed managed care data in response to complaints and inquiries, it is less comfortable using it to build cases against providers and believes that other methods of corroboration are still needed.

C. Claims Payment and Post Payment Review

Post-payment activities, such as audits, are a critical tool in any effective program integrity strategy. The possibility of aggressive claims review, especially when random sampling and the extrapolation of overpayments are used, can be a significant incentive for providers to bill correctly.

The Office of Quality Assurance has 20 auditors who conduct audits on paid claims. Individual staff specialize in various types of service, with a separate pharmacy consultant working on audits of drug claims. An additional two staff, with a third soon to be hired, perform audits of long term care rates. DSS does not audit paid claims from nursing facilities. Rather, it verifies that the costs which go into long term care cost reports are correct and processes financial adjustments when necessary. OQA conducts a full investigation with possible MFCU referrals if fiscal irregularities on a large scale or other types of suspected fraud are found.

In general, OQA demonstrated that it has systems in place to perform the requirements of timely claims payment and post-payment review processes set forth in 42 CFR §§ 447.45(f)(2) and 456.23. Based on data provided to the review team, Connecticut's audit activities led to the following overpayment recoveries in the last three completed SFYs:

SFY	Audit Recoveries	# of Audits	Average Recovery per Audit
2004	$10,420,203	172	$60,583
2005	$6,357,316	158	$40,236
2006	$9,497,057	191	$49,723

DSS confirmed that these figures, averaging nearly $8.8 million per year, are not inflated with third party liability or estate recoveries, which do not accrue through PI activities. Given the number of staff assigned to audit activities and the overall size of Connecticut's Medicaid program, the listed recovery figures suggest an effective system of post-payment review and auditing. However, it should be noted that the reported numbers have not been independently verified.

Audits - Audit activities in Connecticut are conducted concurrently with routine post-payment review of claims and contribute to DSS' recovery totals. Targeted provider audits may arise from post-payment reviews, SURS activities, data mining using the data warehouse, or leads provided through hotline complaints or EOMB feedback. OQA provided the review team with documentation detailing the status of various audits and other projects under its jurisdiction. OQA also conducts reviews of audit findings that are under appeal as well as larger audit projects for provider types of interest. In general, larger audits are conducted at the provider's site allowing direct record reviews. Smaller audits are conducted at the auditor's desk.

D. Interaction with the Medicaid Fraud Control Unit

The Department of Social Services is required under Federal regulations at 42 CFR § 455.15 (a)(1) to refer suspected fraud and abuse cases to the MFCU. The MFCU, in turn, makes a decision about whether to prosecute the provider in question, drop the case for lack of evidence, or refer the case back to OQA for administrative actions. To ensure that problem providers are dealt with effectively and in a timely manner, effective communication and coordination between MFCUs and State Program Integrity Units are essential.

Connecticut's MFCU has existed since 1978 and is located in the Chief State's Attorney's Office. The current director, who has been in his position since 2003, stated that patient abuse was the unit's focus during the first year and a half of his tenure. Recently, provider fraud cases have become the high priority. The MFCU currently has nine professional staff, including four investigators, two forensic fraud accountants and two attorneys. The investigators are Deputy U.S. Marshals, and the accountants have been trained to work with claims data in the Medicaid data warehouse.

Finding: Memorandum of Understanding

The current Memorandum of Understanding (MOU) between DSS and the MFCU has been in effect since 2000. A new MOU is being negotiated and will bring in the HHS Regional Office of Inspector General as a third party. Although OQA currently refers all suspected Medicaid provider fraud cases to the MFCU (and the review team could not find any contrary evidence), the wording of the current MOU obligates OQA to refer only suspected cases of Medicaid provider "criminal" fraud or abuse to the MFCU, with civil referrals made to the Connecticut Attorney General. This wording is in violation of the Code of Federal Regulations at 42 CFR § 455.21(a)(1).

Recommendation

The language in the MOU must be modified to correspond to the regulatory requirement that all potential provider fraud and abuse cases are referred to the MFCU, as is DSS' current practice.

> ***Connecticut Response:*** *The Department has entered into a new MOU with the Chief State's Attorney's Office, Office of the Attorney General and the Office of the Inspector General. The language in this document complies with 42 CFR Sec. 455.21(a)(1).*
>
> **CMS Comment:** *The revised MOU, dated June 2007, satisfies our recommendation.*

Area of Vulnerability: Relationship with the MFCU

The review team conducted separate interviews of OQA staff and the MFCU Director about the quality of interaction between OQA and the MFCU in Connecticut. The team found there have been a significantly low number of Medicaid fraud referrals to the MFCU in recent years. Based on the review of several pieces of MFCU-OQA correspondence and comments from both the MFCU representatives and OQA, the low number of referrals directly relates to a lack of communication and trust between the entities. Although both entities agreed that the successful prosecution of an egregiously fraudulent Medicaid provider would be immensely valuable as a deterrent in Connecticut, they blamed each other with a variety of charges and counter-charges for the lack of cooperation and the inability to develop such cases.

In an HHS/OEI report published in 2007, Connecticut was listed as having the following number of fraud referrals to the MFCU:

Fiscal Year	Referrals to the MFCU
2002-03	45
2003-04	4
2004-05	2

OQA staff stated that there were six referrals to the MFCU in 2005-06. On closer examination, both the MFCU and OQA staff said that the figure of 45 in 2002-03 seemed high. They did not know where it came from and the OQA Director stated that the real figure might have been "4 or 5," rather than 45. Between 2004 and 2006, 14 percent of the MFCU's cases were referred by OQA. In 2005, the figure was 4 percent. OQA reported that 13 cases are currently pending at the MFCU and have been pending for more than two years.

OQA representatives, MFCU staff, and other law enforcement authorities hold quarterly or biweekly meetings. However, it appears that issues or cases raised at these meetings by one entity meet with little follow-up by the other. Both entities acknowledged that communication is largely oral in nature, with minimal written documentation and few expectations for follow-up.

Recommendation
The MFCU and DSS should develop a cooperative and collaborative relationship that furthers the goal of program integrity to the highest extent. They should communicate in writing and document information and referral requests. DSS should be sure that it provides complete hard copy case documentation to the MFCU when referrals are made or requested. In addition, a log of action items from meetings should be maintained and updated as they are completed. Both sides should be clear in their respective expectations for this relationship.

> ***Connecticut Response****: DSS has taken the lead in improving the relationship with the MFCU. DSS has always documented all referrals to the MFCU and maintained responding correspondence from the MFCU. DSS has always provided adequate hard copy case documentation to the MFCU with referrals. The Department disagrees with the recommendation to log action items as the documents are subject to disclosure under the Freedom of Information Act.*

E. Provider Enrollment

EDS is Connecticut's provider enrollment contractor. OQA dedicates one staff person to validate enrollment information. In 2006, OQA screened approximately 5,000 FFS provider applications and denied 85. At any given time, approximately 6,700 FFS providers are enrolled in the Medicaid program representing approximately 29,000 performing providers.

Fee-for-service Enrollment Process – EDS initiates the enrollment process into Connecticut's Medicaid program for most types of FFS providers. EDS sends out enrollment forms and applications for all provider types except nursing homes. Once the package is returned to EDS, it is checked for completeness of forms, accuracy of responses, and for signatures. Copies of licenses are accepted by EDS and passed on to OQA for further review.

EDS does not validate licenses or research disclosure information provided in the application package. The search for individual or entity exclusions and the validity of licenses presented in the application (other than for nursing homes) is performed in OQA. Once an application is approved, the provider is assigned a number and entered into the MMIS provider sub-system.

Out-of-state providers must have their claims approved by the Medical Administration Branch in DSS before the enrollment application is processed. These providers are only enrolled for the date of the service. Some out-of-state providers are required to first provide evidence of enrollment in their home State Medicaid programs or in Medicare before they are allowed to enroll in Connecticut.

DSS re-enrolls all providers every two years by conducting the re-enrollment process for a given segment of providers every month. Pre-printed forms are sent to providers to update information that has changed since initial enrollment or since the last re-

enrollment process. However, providers that do not bill for 12 months are removed from active status by having an end-date placed in their file and are not sent a re-enrollment package. The enrollment agreements also permit the termination of the agreement on 30 days notice without a hearing.

Provider Enrollment in Managed Care - Managed care organizations (MCOs) enroll providers into their own networks through an application or provider agreement process. MCO networks comprise providers and entities under contract with the MCO. Each MCO uses its own process for credentialing and licensing those providers and entities. The contracts that result establish the term of the relationship between the provider or entity with the MCO and the basis for payment, i.e., either capitation or FFS.

The MIG review team met with one of the MCOs, Anthem Blue Cross/Blue Shield Blue Care Family Plan (Anthem), which described its credentialing and licensing process. Providers seeking to contract with Anthem submit an application. Anthem verifies the provider's license and checks on whether there have been any HHS-OIG sanctions, whether there are any limitations on the provider's admitting privileges and insurance coverage, and whether the provider submitted the required disclosure information. If the application is in order, Anthem's credentialing committee approves the application. Anthem searches: a) the HHS-OIG database under the name of any practitioner, b) provider, individual, or facility that has a location in any of the states in which Anthem operates; c) the names of any ancillary providers in the office; d) the Federal employer identification number (EIN); e) the name of the corporation, if any; and f) any references. DSS described the processes of the other three MCOs as being similar to Anthem's.

A provider or entity does not need to be a Medicaid-enrolled FFS provider to contract with a Medicaid MCO. However, in Connecticut, once a provider or entity has been credentialed by an MCO, DSS issues a managed care provider number based on the MCO-provider contractual relationship after contracted managed care plans submit MCO enrollment update forms to EDS. If the forms are incomplete, EDS will notify the MCO. The assignment of Medicaid provider numbers to managed care providers and entities allows DSS to regularly check the full spectrum of providers across delivery systems for exclusions, but it does not give providers access to both delivery systems. If a managed care provider or entity does not have a FFS provider number, it may not submit a FFS claim directly to DSS.

DSS contracts with an external quality review organization (EQRO), Mercer Government Human Services Consulting (Mercer), which conducts a review of a random sample of files for each MCO to verify the MCO's credentialing process.

Nursing Homes - The Connecticut Department of Public Health sends out nursing home application packages, validates licenses and performs site visits. Applications are sent to the Medical Care Operations Branch in DSS for enrollment processing along with the Medicare/Medicaid Certification and Transmittal forms (CMS Form 1539) filled out by the survey agency. This branch does not search for exclusions of the entity or any of the individuals associated with it. The review team was told that these applications will go to

OQA once the new MMIS is in place. Once approved, the nursing home information is entered into the MMIS provider subsystem.

Provider Application Validations and Exclusion Searches - The procedures at DSS to validate application information and search for exclusions appear to be efficient and fairly thorough. The applications are sent in batches from EDS and entered by OQA into the application database. If any information is missing in new enrollment applications, the application is denied and sent back to the provider. If a durable medical equipment (DME) supplier application does not have a Medicare number, DSS staff visit the DME supplier's location. The individual who conducts the validation process utilizes the following search techniques when necessary:

- Department of Labor records are searched to see if the company associated with the excluded individual is a Medicaid provider in Connecticut.
- Licensing Boards are contacted to determine if the license is current or if any actions have been taken against it. However, this is not always done for out-of-state providers.
- Record searches through ChoicePoint, an information vendor, include verifying a Social Security Number (SSN) and other personal identifiers, business affiliations, license information, disciplinary actions, and sanctions in the Medicare Exclusions Database (MED) or by HHS-OIG and the General Services Administration (GSA). ChoicePoint is the only source for the identification of GSA debarment information.

The Office of Quality Assurance compares the application database (including approved and denied applications since 1998) by EIN and SSN to the MED on a weekly basis. Any identified matches result in denied applications. OQA retains this information in the application database in the event the provider or officer submits another enrollment application. On a monthly basis, EDS compares the MED to the MMIS provider database kept by EDS to identify individuals and entities that become excluded after being enrolled. This search is also performed by EIN and SSN. EDS reports any findings to OQA.

Finding: Notification to HHS-OIG

While the frequency of the Department's exclusion screenings is a noteworthy practice, DSS does not have a policy to report to HHS-OIG any action it takes on the provider's application for participation in the program, as required at 42 CFR § 1002.3(b). These actions include suspension, settlement agreements, and situations where the provider withdraws from the program to avoid a formal sanction. [2]

[2] One regulatory finding from the draft report provided to the State has been deleted from this final report. Connecticut does have a State plan amendment on file with CMS Region I with the assurances required by 42 CFR § 1002.100.

Recommendation
Develop and implement policies and procedures to report to the HHS-OIG appropriate disclosure information and adverse actions that DSS takes on a provider's application for participation.

> ***Connecticut Response:*** *The Department disagrees with your interpretation 42 CFR Sec. 455.106 (b)(2). This CFR pertains only to "persons convicted of a crime" and your finding expands the actions covered by this CFR to actions not necessarily related to a criminal conviction.*
>
> *The Department will comply with your recommendation to report appropriate disclosure information to HHS-OIG, but only as required by the CFR. Additionally, the State Plan will be amended as needed.*
>
> **CMS Comment:** *In the draft report provided to the State, CMS referred to 42 CFR § 455.106(b)(2) and cited Connecticut for its failure to have policies and procedures related to reporting adverse actions taken against providers. CMS is seeking an official opinion from the Office of General Counsel on whether 42 CFR § 455.106(b)(2) applies here.*
>
> *Nonetheless, an OIG regulation at 42 CFR § 1002.3, entitled "Disclosure by providers and State Medicaid agencies" addresses the notification requirement more directly by requiring States to report any action taken to limit the ability of a provider or entity to participate. Consequently, in this final report, we are citing this regulation as the basis for the CMS finding.*

F. Disclosure
States must not only require that certain related information be disclosed, but they must also use it to search for excluded individuals and entities trying to enroll in their Medicaid program. Additionally, States must report criminal conviction disclosures and the identity of State-sanctioned individuals to HHS-OIG for possible Federal exclusions.

Managing Employee Disclosure - EDS and OQA staff ensure that provider, owner, and officer information (including EIN/SSN) is captured on enrollment forms and in the DSS Application Database. However, managing employee information is not captured on any of Connecticut's provider applications.

Similarly, managed care provider applications and agreements require that providers disclose information specific to the individual provider. If an entity is seeking to contract with an MCO, the MCO solicits identity information about the entity during the credentialing process. Two of the four MCOs fail to capture managing employee information. Wellcare of Connecticut, Inc./FirstChoice Health Plan (Wellcare) solicits information on the authorized representative of ancillary/health care delivery organizations. Although Anthem requires information on the office manager in its provider application for entities, it does not search the HHS-OIG database for owners of provider entities.

Area of Vulnerability: Disclosure of Managing Employee Information

Although providers are required to disclose the identities of managing employees who have been convicted of a health care-related offense, the identities of all managing employees are not captured in either the FFS or managed care enrollment processes. As a result, DSS cannot ensure that providers or entities billing the Medicaid program do not employ individuals who may be excluded from the program or who have criminal convictions and must be excluded.

Recommendation

Ask for managing employee information on all enrollment forms or in some manner on attachments to those forms and require through MCO contracts that MCOs solicit managing employee information from providers and entities in the credentialing process. This information should also be captured in the application database for comparison during the enrollment process and routinely thereafter.

> ***Connecticut Response:*** *42 CFR does not provide a definition what a managing employee is. Therefore it is difficult to comply with the recommendation. The Department has taken specific actions to ensure that enrolled providers screen all of their employees for exclusion actions.*
>
> **CMS Comment:** *"Managing Employee" is defined at 42 CFR § 455.101 as "a general manager, business manager, administrator, director, or other individual who exercises operational or managerial control over, or who directly or indirectly conducts the day-to-day operations of an institution, organization or agency."*

Referral of Disclosure Information - The HHS-OIG must have the necessary information to consider excluding an individual or entity. The HHS-OIG gathers this information from a variety of sources including State Medicaid agencies. Federal regulations at 42 CFR § 455.106(b)(1) require States to inform the HHS-OIG of criminal conviction information disclosed during the provider enrollment or re-enrollment processes.

Finding: Notification to HHS-OIG

DSS does not have a policy to refer criminal conviction information to the HHS-OIG as required in 42 CFR § 455.106(b)(1). The identity of any person who is an owner or managing employee and has been convicted of a criminal offense related to involvement in any program under Medicaid or Title XX must be reported to the HHS-OIG within 20 working days.

Recommendation

Develop and implement policies and procedures to ensure the timely referral of criminal conviction information to the HHS-OIG.

> ***Connecticut Response:*** *Similar to the previous finding, the Department will comply with the recommendation to implement policies and procedures to ensure timely referral of criminal conviction information to HHS-OIG and amend the State Plan as necessary. However, the Department notes that this requirement only pertains to information obtained through the provider application process.*

Area of Vulnerability: Policies and Procedures

In reviewing Connecticut's program integrity and provider enrollment practices, the review team observed that relatively few written policies and procedures were available. Although OQA provided four or five policies and procedures to the review team on-site, not all of these policies and procedures were dated and there was no indication of whether they were current. The absence of codified policies and procedures represents a potentially serious vulnerability in the event DSS loses experienced PI or provider enrollment staff or is called upon to defend its processes.

Recommendation

The Department of Social Services should develop, compile, and update policies and procedures covering all of its program integrity processes.

> ***Connecticut Response****: The Department agrees that it is important to adequately document its program integrity processes and will take the appropriate steps to do so.*

G. Managed Care

In Connecticut, the DSS Medical Services Administration oversees the managed care program. DSS currently contracts with four MCOs to provide medical services to 76 percent of the State's Medicaid population, although this population currently accounts for approximately 17 percent of total State Medicaid outlays. DSS' Medicaid managed care contracts were last competitively procured in 1997. Since that time, DSS has issued new contracts or extended those in force. The current contract term is August 11, 2001 through June 30, 2007. At the time of the review, DSS planned to extend the current contract term and anticipates it will competitively procure the contracts again next year.

The MCOs currently under contract with DSS are Anthem, Community Health Network of Connecticut, Inc., Wellcare, and Health Net of Connecticut, Inc. The contracts are full-risk capitated contracts providing all services under the Medicaid program, except behavioral health, which was carved out in January 2006. Providers contract with the MCOs. Specialists are paid on a FFS basis and primary care physicians (PCPs) are paid through capitation, although there has been an increasing trend toward FFS reimbursement of PCPs as well.

DSS' model MCO contract contains several provisions regarding credentialing, identifying excluded providers, detecting and preventing fraud and abuse, and referral of potentially fraudulent or abusive activity. Specifically, the contract provides that MCOs must:

- Not employ or contract with any provider excluded under section 1128 or 1128A (section 3.09(g))
- Include in provider contracts the exclusion of any provider that has been suspended from Medicare or Medicaid in any state (section 3.11(g))
- Verify that providers have not been suspended or terminated from Medicare or Medicaid (section 3.12(b)(2))
- Immediately notify DSS when the MCO detects potential fraud and abuse (section 3.51(d))
- Have administrative and management procedures and a mandatory compliance plan to guard against fraud and abuse (section 3.51(g))
- Examine publicly available data including the MED and List of Excluded Individuals/Entities (section 3.51(h))
- Provide the identity of each person or corporation with an ownership or controlling interest of 5% (section 3.51(i))
- Provide complete information when the MCO becomes aware of any employee or subcontractor convicted of a civil or criminal offense related to Medicare or Medicaid (section 3.51(j))
- Comply with all State and Federal laws and rules (section 5.15)

Recipient Verification Procedure/Managed Care - Just as Federal regulations require that State Medicaid programs ascertain whether FFS providers perform the services for which they are billing, States are responsible for verifying whether Medicaid managed care enrollees receive the covered services that their MCO providers claim to have furnished in accordance with MCO contracts. In its managed care contracts, DSS delegates to the MCOs the obligation to verify receipt of services. Though DSS' managed care chief stated that MCOs issue EOMBs, the contract does not require that MCOs issue EOMBs to managed care enrollees. The review team met with one of the MCOs, Anthem, which stated that it never sends out EOMBs.

During the program integrity review CMS conducted in October 2001, CMS noted that the managed care unit should add language to the managed care contracts "that implements a process to verify with the recipient that services rendered by a MC [managed care] provider were received." During the current review, the review team asked how DSS verifies that enrollees receive managed care services. DSS responded that MCOs are required to report on service utilization in encounter data reports. The MCO contract requires MCOs to submit encounter data that will be reviewed by Mercer.

In the course of its annual reviews, Mercer examined a sample of up to 100 encounters from each MCO to evaluate the performance of their contractual obligations. While Mercer reviewed encounter data in relation to the MCOs' meeting six performance measures, none of these was for the specific purpose of verifying enrollees' receipt of services from the MCO providers. Mercer also reviewed the adequacy of encounter data systems in enabling plans to manage the delivery of health care services to enrollees. In 2004, Mercer found that encounter data systems were generally good, despite noting in

the same report that the encounter data were not complete and that the systems had numerous limitations. Results in 2005 and 2006 were similar to those in 2004.

Area of Vulnerability: Recipient Verification Procedure

DSS does not utilize encounter data to verify receipt of managed care services and uses no other means for determining whether managed care enrollees receive managed care services from MCOs.

Recommendation

Require the EQRO to evaluate encounter data to review enrollees' receipt of managed care services. Alternately, require MCOs to issue EOMBs to enrollees and to provide EOMB data to DSS.

> ***Connecticut Response:*** *The Department is reviewing this recommendation and does not have a response at this time.*
>
> **CMS Comment:** *We request this response within 60 days of Connecticut's receipt of this final report.*

EQRO Monitoring - DSS and its fiscal agent, EDS, have mechanisms in place that, with some limitations, are effective in capturing provider enrollment and disclosure information within the existing MMIS. Beyond this, however, DSS' direct oversight of the managed care program is limited. Mercer performs the bulk of contract monitoring activities and reviews each MCO annually. Under the EQRO contract, Mercer is to conduct a comprehensive review of each MCO during the first year of the contract and follow up reviews of each MCO during each of the two remaining years of the contract. If a review results in no recommendations, Mercer would not necessarily assess whether an MCO meets a performance measure in a subsequent review.

During the 2004 review, Mercer assessed whether the MCOs met specified fraud and abuse criteria. Mercer found that each of the four MCOs had defined and written fraud and abuse policies and procedures, including: a) annual staff training; b) a process in place that ensured payments were not made to excluded providers; c) a credentialing process that documented the provider's eligibility to participate in the Medicaid program; and d) a defined process for reporting fraud and abuse. Two of the four MCOs, Anthem and Health Net, were able to quantify dollar savings as a result of fraud and abuse investigations and had reported fraud and abuse to DSS during 2004.

One MCO, Community Health Network, did not have an active SURS or a process for comparing provider utilization patterns and did not make provider office visits part of the credentialing process. One recommendation resulted from these unmet criteria: the MCO should expand its current system capabilities for fraud and abuse.

Area of Vulnerability: EQRO Contract Monitoring

Despite Mercer's 2004 findings concerning Community Health Network, its 2005 and 2006 reviews did not follow up on whether corrective action was taken to address this

problem. In fact, they did not address fraud and abuse issues at all. There does not appear to be a consistent annual review and evaluation of the activities undertaken by Connecticut's Medicaid MCOs to prevent and detect fraud and abuse.

Recommendation
Require the EQRO to assess MCOs for fraud and abuse compliance during each annual review.

> ***Connecticut Response:*** *The Department agrees with the need to insure that the MCO's meet fraud and abuse contract requirements and will review its monitoring steps with Mercer.*

Managed Care Contract Enforcement - The MCO contract requires MCOs to report instances of suspected fraud and abuse to OQA. The MCO contract does not require reporting in a specific format or require reporting on a regular schedule. While Mercer found in 2004 that each of the MCOs had a defined process for reporting fraud and abuse, only two of the MCOs had reported fraud and abuse to OQA during 2004.

The review team met with Anthem, one of the two MCOs with such a defined process. Although Anthem reported it kept a record of complaints, it stated there were not many complaints regarding fraud and abuse. However, Anthem was unable to cite specific statistics. There is no set protocol for referring matters of suspected fraud and abuse. Moreover, when fraud and abuse issues arise, Anthem does not routinely direct referrals to OQA, as is contractually required. Rather, the plan may refer cases directly to the MFCU, HHS-OIG, or other law enforcement agencies. When asked if it could provide examples of referrals that had been made to OQA, the MFCU, or another law enforcement agency, Anthem reported that it has no dedicated fraud and abuse complaint file and that referrals are usually made orally by telephone.

Area of Vulnerability: Managed Care Contract Enforcement
The Department of Social Services does not require regular MCO reporting of fraud and abuse complaints and action taken on complaints and so is unable to quantify or trend the fraud and abuse complaints made in the managed care program. Consequently, DSS is unable to enforce the MCO contract against an MCO that violates the referral requirements.

Recommendation
Require MCOs to regularly report fraud and abuse complaints and actions the MCOs have taken on those complaints.

> ***Connecticut Response:*** *The Department will consider amending future contracts to require the reporting of fraud and abuse.*

III. CONCLUSION

Many of the State of Connecticut's program integrity efforts are effective. Over the last three years, the DSS has conducted an annual average of 174 audits and recovered $8.8 million in overpayment on average each year. It is in compliance with most Federal regulations regarding program integrity and fraud and abuse. DSS also operates a strong data mining operation and closely monitors for excluded providers. CMS encourages DSS to continue its commendable practices and look for additional opportunities to improve the overall fiscal and program integrity of the program.

The three findings on non-compliance with Federal regulations relate to fraud referrals and provider enrollment and monitoring issues. Each finding should be addressed immediately. It is imperative that DSS come into compliance with Federal program integrity regulations as soon as possible.

CMS encourages DSS to closely examine each identified area of vulnerability as well. DSS' relationship with the MFCU, DSS' MCO fraud and abuse procedures and its own documentation of program integrity procedures all need attention as well. While DSS is not obligated to follow CMS' recommendations, it will considerably strengthen its overall efforts if it does so.

Unfortunately, the poor relationship between DSS and the MFCU is singularly noteworthy. The readily apparent lack of trust and effective communication adversely affects the effectiveness of Medicaid program integrity efforts in Connecticut. It is hard to imagine that either DSS or the MFCU could be considered to be completely effective in this area until such time as they successfully address these problems.

The Medicaid Integrity Group looks forward to working with the State of Connecticut on correcting its findings, eliminating its areas of vulnerability, and building on its commendable practices.

Appendix A – DSS Response to Draft Report

September 5, 2007

Robb Miller
Director of Field Operations
Medicaid Integrity Group
Centus [sic] for Medicare and Medicaid Services

RE: Review of Program Integrity Procedures

Dear Mr. Miller:

Thank you for providing a draft of the above referenced report and allowing me to comment on its content. The report identifies four Federal regulatory findings and six areas of vulnerability. I have organized my response to first address each finding and then each area of vulnerability. In addition, I have noted some statements in the report that do not accurately represent the operations of this Department.

Findings

Memorandum of Understanding

The Department has entered into a new MOU with the Chief State's Attorney's Office, Office of the Attorney General and the Office of the Inspector General. The language in this document complies with 42 CFR Sec. 455.21(a)(1). A copy of the document is attached.

State Plan Exclusion Authority

The Department agrees with the recommendation to amend the State Plan to include State Exclusion Authority.

Notification to HHS-OIG

The Department disagrees with your interpretation 42 CFR Sec. 455.106 (b)(2). This CFR pertains only to "persons convicted of a crime" and your finding expands the actions covered by this CFR to actions not necessarily related to a criminal conviction.

The Department will comply with your recommendation to report appropriate disclosure information to HHS-OIG, but only as required by the CFR. Additionally, the State Plan will be amended as needed.

Notification to HHS-OIG

Similar to the previous finding, the Department will comply with the recommendation to implement policies and procedures to ensure timely referral of criminal conviction information to HHS-OIG and amend the State Plan as necessary. However, the Department notes that this requirement only pertains to information obtained through the provider application process.

Areas of Vulnerability

Relationship with the Medicaid Fraud Control Unit (MFCU)

DSS has taken the lead in improving the relationship with the MFCU. DSS has always documented all referrals to the MFCU and maintained responding correspondence from the MFCU. DSS has always provided adequate hard copy case documentation to the MFCU with referrals. The Department disagrees with the recommendation to log action items as the documents are subject to disclosure under the Freedom of Information Act.

Disclosure of Managing Employee Information

42 CFR does not provide a definition what a managing employee is. Therefore it is difficult to comply with the recommendation. The Department has taken specific actions to ensure that enrolled providers screen all of their employees for exclusion actions.

Policies and Procedures

The Department agrees that it is important to adequately document its program integrity processes and will take the appropriate steps to do so.

Recipient Verification Procedure

The Department is reviewing this recommendation and does not have a response at this time.

EQRO Contract Monitory

The Department agrees with the need to insure that the MCO,s [sic] meet fraud and abuse contract requirements and will review its monitoring steps with Mercer.

Managed Care Contract Enforcement

The Department will consider amending future contracts to require the reporting of fraud and abuse.

Technical Corrections

Page 3 "Administrative Action"

The Office of the Attorney General does not have a "civil division." The Office is the civil division of the State's judicial branch.

Page 4 "Providers targeted by OQA receive written notification when an action is initiated."

This only related to the suspension of providers from the Medicaid program.

Page 5 "While EDS manages the resource and provides tools…"

DSS actually manages the data warehouse. EDS manages the operation of the data warehouse.

Page 6 "review the work that Craig J. Lubitski Consulting does in processing rates and audit reports for nursing home"

OQA does not review the rate setting processes by Lubitski. The referenced staff actually perform audits of long term care rates.

If you have any questions concerning the above comments,
please contact me at (860) 424-5903.

Sincerely,

James Wietrak

cc: David Parrella
John McCormick

Appendix B – List of Acronyms

CMS	Centers for Medicare and Medicaid Services
DME	Durable Medical Equipment
DSS	Department of Social Services
EDS	Electronic Data Systems
EIN	Employer Identification Number
EOMB	Explanation of Medical Benefits
EQRO	External Quality Review Organization
FFS	Fee-For-Service
FTE	Full-Time Employee
GSA	Government Services Administration
HHS-OIG	Department of Health and Human Services Office of the Inspector General
MAR	Management and Administrative Reporting
MCO	Managed Care Organization
MED	Medicare Exclusions Database
MFCU	Medicaid Fraud Control Unit
MIG	Medicaid Integrity Group
MMIS	Medicaid Management Information System
MOU	Memorandum of Understanding
OQA	Office of Quality Assurance
PCP	Primary Care Physician
PI	Program Integrity
SCHIP	State Children's Health Insurance Program
SFY	State Fiscal Year
SSI	Supplemental Security Income
SSN	Social Security Number
SURS	Surveillance and Utilization Review Subsystem