



Vulnerabilities and Mitigation Strategies in Medicaid Personal Care Services

Medicaid Integrity Institute
Center for Program Integrity
Centers for Medicare & Medicaid Services
February 2018¹



¹ Updated from preliminary paper dated November 2017.

Executive Summary

Personal Care Services for elderly or disabled Medicaid beneficiaries who need assistance with Activities of Daily Living are often critical for beneficiaries to enjoy the greater independence of living in their homes instead of in a nursing facility or other institution. However, because Personal Care Services (PCS) are provided by caregivers typically working without direct supervision in beneficiaries' homes, Medicaid program integrity stakeholders have expressed growing concern that significant vulnerabilities exist in program safeguards to protect beneficiaries as well as Medicaid funds. PCS pose special challenges of ensuring beneficiary safety from neglect, abuse, or theft and preventing improper Medicaid payments due to billing for services not rendered and other forms of fraud, waste, or abuse.

To discuss these vulnerabilities and develop more effective mitigation strategies, the Centers for Medicare & Medicaid Services (CMS) assembled a body of experts at the Medicaid Integrity Institute (MII) for a course entitled, "Emerging Trends in Home and Community-Based Services and Personal Care Services" in February 2017. Program integrity experts from State Medicaid Agencies, state Medicaid Fraud Control Units, state Inspectors General, CMS, the Department of Justice, and the Department of Health and Human Services (HHS) Office of Inspector General (OIG) brought their respective areas of expertise to bear on addressing these important issues. This paper provides an account of the consensus recommendations developed by MII participants to help states more effectively protect vulnerable beneficiaries and reduce improper payments in PCS.

The discussion of MII participants centered on identifying vulnerabilities of beneficiary harm, fraud, waste, and abuse—and mitigations to address those vulnerabilities. Many of the mitigation strategies discussed by MII participants and presented in this paper have already been adopted in some state Medicaid programs. The purpose of this paper is to provide and disseminate a compendium of the program integrity vulnerabilities and mitigation strategies in PCS shared by MII participants to inform Medicaid programs nationwide.

Working together, Medicaid stakeholders from state Medicaid agencies, state Medicaid Fraud Control Units, state Inspectors General, as well as their federal partners in CMS and the HHS-OIG, can use this compendium to implement mitigation strategies identified by MII participants to minimize the risk to beneficiaries and to reduce improper payments in PCS:

- Ensure only screened and qualified providers oversee or provide care to beneficiaries
- Approve eligible beneficiaries for services appropriate to their needs
- Ensure services are fully and accurately documented
- Require claims to include complete specifications regarding services
- Optimize prepayment review to prevent improper payments
- Improve data analytics to reveal billing anomalies
- Improve investigations and audits to identify and recover improper payments
- Use administrative actions to sanction bad actors
- Streamline referral and investigation of suspected fraud
- Implement parallel safeguards in managed care contracts

Table of Contents

Executive Summary	1
Introduction.....	3
Relative Costs and Benefits of Long-Term Care Delivery Systems.....	3
Personal Care Services.....	4
Broad Risks in Personal Care Services	5
Harm to Beneficiaries	5
Loss of Medicaid Funds through Fraud, Waste, or Abuse	6
Organization of the Paper	7
Strategic Goals Identified by MII Participants	8
Prevention and deterrence activities protect beneficiaries and safeguard taxpayer funds	9
Ensure only screened and qualified providers oversee or provide care to beneficiaries	9
Approve eligible beneficiaries for services appropriate to their needs.....	18
Ensure services are fully and accurately documented	20
Require claims to include complete specifications regarding services.....	22
Optimize prepayment review to prevent improper payments.....	23
Post-payment review can recover improper payments and identify fraud	25
Improve data analytics to reveal billing anomalies.....	25
Improve investigations and audits to identify and recover improper payments	27
Use administrative actions to sanction bad actors	30
Streamline referral and investigation of suspected fraud.....	32
Personal care services in Medicaid managed care	34
Implement parallel safeguards in managed care contracts	34
Closing Remarks.....	34

Introduction

Home and Community-Based Services (HCBS) serve critical needs for Medicaid beneficiaries who are elderly or disabled. But concern is growing among Medicaid program integrity stakeholders that significant vulnerabilities exist in program safeguards to protect beneficiaries and to prevent Medicaid improper payments for these services. There are risks of potential harm to beneficiaries from abuse, neglect, or theft perpetrated by unscreened or unqualified attendants working without direct supervision in beneficiaries' homes. The risk of improper payments in HCBS due to billing for services not rendered and other forms of fraud, waste, or abuse is also significant due to inadequate assessments, poor documentation, difficulties in verifying services, outright fraud, and other vulnerabilities.

To assemble a body of experts to discuss these vulnerabilities and develop more effective mitigation strategies, the Centers for Medicare & Medicaid Services (CMS) held a course entitled, "Emerging Trends in Home and Community-Based Services and Personal Care Services (PCS)" at the Medicaid Integrity Institute (MII) in early February 2017.² A group of 76 program integrity experts came together from State Medicaid Agencies (SMAs), state Medicaid Fraud Control Units (MFCUs), state Inspectors General, CMS, the Department of Justice (DOJ), and the Department of Health and Human Services (HHS) Office of Inspector General (OIG). Representatives from these organizations brought clinical, program integrity, policy, operations, social work, law enforcement, and programmatic expertise to bear on addressing these important issues.

The diverse structure of MII participants engendered a vigorous discussion of vulnerabilities, mitigation strategies, challenges, and barriers related to HCBS/PCS administration, and led to the development and articulation of a holistic approach to HCBS/PCS program integrity. As a result, the MII participants reached consensus on numerous program improvements that can advance the safe delivery of services to vulnerable populations of beneficiaries receiving PCS and provide more effective stewardship of program funds. This paper provides a written account of the consensus recommendations developed by MII participants to help states more effectively protect vulnerable beneficiaries and reduce improper payments in PCS.

Relative Costs and Benefits of Long-Term Care Delivery Systems

Individuals who are elderly or disabled comprised 23 percent of the Medicaid population but accounted for 55 percent of Medicaid expenditures in federal fiscal year (FFY) 2015. Over half of expenditures for elderly and/or disabled Medicaid beneficiaries were for Long-Term Services and Supports (LTSS), accounting for 30 percent of total Medicaid expenditures in FFY 2015. Concerted efforts by CMS and states over the past 20 years have shifted LTSS for individuals who are elderly and/or disabled away from primarily institutional care to expand the share of

² Through the MII, CMS provides training to state program integrity staff at no cost to states in collaboration with the Department of Justice's National Advocacy Center Office of Legal Education in Columbia, South Carolina and through distance learning webinars.

HCBS. Institutional care accounted for over 80 percent of LTSS expenditures until 1997, but only 45 percent of LTSS expenditures in FFY 2015.^{3,4}

The shift of LTSS from institutional care to HCBS has demonstrated considerable cost-effectiveness: at approximately the same cost, over twice as many Medicaid beneficiaries were served with only HCBS as were served by only institutional care in calendar year 2013.⁵ While costs for long-term care for the aging “baby boom” population are escalating, the considerable savings of HCBS/PCS over institutionalized care are compounded by the consideration that—although PCS are not strictly medical costs—PCS can replace, prevent, or delay the incursion of medical costs.

More importantly, HCBS offer clear benefits for the individual beneficiary over institutionalized care. Individuals benefit from enjoying greater choice and independence with care in their homes. HCBS programs empower individuals to have more control over their daily lives and the management of their health. In January 2014, CMS promulgated a final rule that requires HCBS waiver services to include a person-centered planning process that reflects cultural considerations of the individual and provides information in plain language that is accessible to individuals with disabilities and to persons with limited English proficiency. Other HCBS state plan and waiver authorities also provide states with the option to offer self-directed HCBS—services that are planned and purchased under the direction and control of the individual.⁶ Program integrity considerations in this paper, as important as they are, should not overshadow considerations of respect for the dignity of the individual and the individual’s choice and control over decisions regarding his or her care.⁷

Almost three million Medicaid beneficiaries received services in 2013 through the three main Medicaid HCBS programs at that time: the home health services state plan benefit, the personal care services state plan benefit, and section 1915(c) HCBS waivers. By 2015, more than 640,000 people were on section 1915(c) waiver waiting lists, with the average waiting time exceeding two years.⁸ Home health, PCS, and other HCBS programs are offered under different statutory authorities with varying requirements. With the exception of the home health benefit, the January 2014 final rule harmonized many requirements across HCBS programs.

Personal Care Services

Personal Care Services are provided for individuals who need assistance with Activities of Daily Living (ADL) such as bathing, dressing, toileting, ambulation, or feeding. Personal Care Services can also include assistance with Instrumental Activities of Daily Living (IADL) such as meal preparation, grocery shopping, and money management. These services are provided by Personal Care Attendants (PCAs) who typically work for PCS agencies, but in some programs can provide care as individual attendants who contract with the state directly or through a fiscal intermediary, or are hired by the beneficiary in self-directed care delivery. PCS provide a large

³ CMS, [2016 Actuarial Report on the Financial Outlook for Medicaid](#).

⁴ Eiken, S. et al, [Medicaid Expenditures for Long-Term Services and Supports \(LTSS\) in FY 2015](#), April 2017.

⁵ Ibid; Eiken, S., [Medicaid Long-Term Services and Supports Beneficiaries in 2013](#), September 2017.

⁶ [79 FR 2948](#), January 16, 2014.

⁷ CMCS Informational Bulletin, [Strengthening Program Integrity in Medicaid Personal Care Services](#), December 13, 2016.

⁸ Ng, T. et al, [Medicaid Home and Community-Based Services Programs: 2013 Data Update](#), October 2016.

portion of the services that allow beneficiaries to remain living in their homes or community instead of in a nursing facility or other institution.

Broad Risks in Personal Care Services

The mandate of any program integrity organization is fundamentally one of protection: to minimize the risk of harm to the program's beneficiaries and to ensure that the resources deployed for their care are used appropriately for providing care—not misdirected into fraud, waste, or abuse. External agents pose threats to the program—bad actors who may harm beneficiaries or misdirect program funds to enrich themselves, as well as irresponsible actors who may waste or abuse program funds. Because of such threats, the program faces risk:

- *Risk—the potential for harm to beneficiaries or loss of program funds*

Harm to Beneficiaries

The first risk to consider in Medicaid PCS is harm to beneficiaries. Because PCS are provided by caregivers typically working without direct supervision in the beneficiary's home, risks to the beneficiary range from inadequate care or theft, to neglect, as well as physical or emotional abuse. The potential for risk is increased if PCS agencies employ attendants who are not screened or not sufficiently trained and/or supervised to provide the needed care to their clients. More direct threats can result from attendants who provide substandard care, neglect the needs of their clients, steal their personal belongings or medications, intimidate clients to prevent them from reporting improper practices or offenses, threaten clients with emotional abuse, or physically harm beneficiaries.

Examples of Abuse or Neglect of Medicaid Beneficiaries by Personal Care Attendants

The HHS-OIG has investigated and reported cases of neglect and abuse of Medicaid beneficiaries by PCS attendants, including especially egregious cases such as:

- a beneficiary with developmental disabilities left in distress in a locked car on a hot July day while the PCA was shopping with a companion (Maryland);
- a beneficiary left for a week in an incoherent state, covered in dried excrement (Illinois);
- a beneficiary living in filth and suffering severe dehydration and malnourishment necessitating hospitalization as a result of a caregiver's neglect (Idaho); and
- a beneficiary dying of exposure to cold due to inadequate supervision by a PCA (Pennsylvania).⁹

⁹ OIG, [Investigative Advisory on Medicaid Fraud and Patient Harm Involving Personal Care Services](#), October 3, 2016.

Government agencies, including staff who have oversight of those who place attendants in beneficiaries' homes or who implement the mandate of program integrity efforts, have a duty to ensure that all reasonable measures have been taken to screen, qualify, and train individual caregivers so beneficiaries remain safe and are treated respectfully, and the care they need is provided in accordance with program rules.

Loss of Medicaid Funds through Fraud, Waste, or Abuse

The risk of improper payments in PCS due to billing for services not rendered and other forms of fraud, waste, or abuse is considerable. The Medicaid fee-for-service improper payment rate for the claim category of personal support services (which includes PCS and other services)¹⁰ was projected as 17.4 percent by CMS's Payment Error Rate Measurement (PERM) program for the 2016 national rolling rate. This improper payment rate translates to a projected \$4.7 billion of improper payments for personal support services.¹¹

It should be noted that identified improper payments should *not* be confused with fraud or even always considered as expenses for services that should never have been billed or paid. An improper payment is defined as any payment that should not have been made or that was made in an incorrect amount (including underpayments as well as overpayments) under legally applicable requirements or where documentation is missing or not available. The errors contributing to the 2016 PERM improper payment rate for personal support services were primarily due to incomplete or no documentation, providers not screened as required by federal regulations, and pricing errors.¹²

While fraud may not be the cause of most improperly paid claims, fraud does occur in PCS as well as in other health care services. While most PCS providers and beneficiaries are honest, PCS fraud often comes from unscrupulous agencies or attendants who falsify timesheets to bill for services not provided. Providers may coerce or collude with beneficiaries to sign false or blank timesheets, sometimes splitting the payments for services not provided with beneficiaries as an inducement to collusion. Several cases have been prosecuted where an attendant falsely claimed to have provided care, e.g., when working a full-time job or when the attendant or beneficiary was out of the country.¹³ In addition, some unscrupulous providers and/or beneficiaries may conspire to obtain authorization for services not needed or for a higher level of services than needed, which may involve coaching beneficiaries on how to feign or exaggerate disabilities. Sometimes PCS agencies pay kickbacks to independent attendants to join the agency and split the higher Medicaid payment to the agency, increasing costs for the same services provided by the same caregivers.

¹⁰ CMS, [Payment Error Rate Measurement Manual](#), January 2017. Personal Support Services is the PERM claim category that includes PCS, as well as targeted case management, private duty nursing, midwife, homemaker, respite, and meal delivery services.

¹¹ CMS, [Medicaid and CHIP 2016 Improper Payments Report](#), November 2016. The 2016 national rolling improper payment rate includes findings from the most recent three PERM measurements (2014, 2015, and 2016) to reflect findings for all 50 states and the District of Columbia.

¹² Ibid.

¹³ OIG, [Investigative Advisory on Medicaid Fraud and Patient Harm Involving Personal Care Services](#), October 3, 2016.

Waste or abuse can occur when inadequate assessment practices lead to approval of unneeded services, or caseworkers succumb to outside pressure to approve more services than needed. Sometimes beneficiaries or their family members may “shop” PCS agencies to find one that will obtain authorization for more services or pay a family member more to provide care in programs where family care can be paid for by Medicaid.

These threats of fraud, waste, and abuse pose a significant risk of loss of Medicaid funds to enrich unscrupulous individuals, while denying the use of those funds to provide care to those in need and driving up the cost to taxpayers. Again, government agencies that have oversight of Medicaid PCS have a responsibility to develop and implement effective policies and procedures to protect Medicaid funds against misdirection into fraud, waste, and abuse.

Organization of the Paper

The discussion of MII participants centered around identifying vulnerabilities of PCS to fraud, waste, and abuse, and mitigations to address those vulnerabilities.

- *A Vulnerability is a specific weakness in the program or a gap in protection efforts that can be exploited by bad actors, resulting in the risk of potential harm or loss being realized.*

While external threats cannot be eliminated from the world, we can work together to shore up the vulnerabilities in the program—to strengthen the weaknesses and close the gaps.

- *A Mitigation is an action that reduces the risk by helping to remedy the vulnerability—an action to correct the weakness, preventing the risk from being realized, and thus fulfilling the program integrity mandate of protection.*

Many of the consensus recommendations developed by MII participants to help states minimize the risk of harm to beneficiaries and reduce improper payments are already being implemented in some states with measurable success. Because of the strong emphasis in these recommendations on prevention, states can expect a significant return on investment by implementing these mitigation strategies for both beneficiary welfare and Medicaid savings. Working together, Medicaid stakeholders from state Medicaid agencies, state Medicaid Fraud Control Units, state Inspectors General, as well as their federal partners in CMS and the HHS-OIG, can improve on the implementation of these mitigation strategies to protect beneficiaries from harm and to reduce improper payments in HCBS/PCS.

A number of strategic goals arose from MII participants’ discussion of vulnerabilities and recommended mitigations. The body of this paper is organized by sections for each of the following strategic goals. In each section, vulnerabilities undermining the goal are discussed, followed by recommended mitigations to address those vulnerabilities. This approach is consistent with the practices identified in the framework for managing fraud risks developed by the Government Accountability Office (GAO).¹⁴

¹⁴ GAO, [A Framework for Managing Fraud Risks in Federal Programs](#), GAO-15-593SP, July 2015.

Strategic Goals Identified by MII Participants

Prevention and deterrence activities protect beneficiaries and safeguard taxpayer funds

- Ensure only screened and qualified providers oversee or provide care to beneficiaries
- Approve eligible beneficiaries for services appropriate to their needs
- Ensure services are fully and accurately documented
- Require claims to include complete specifications regarding services
- Optimize prepayment review to prevent improper payments

Post-payment review can recover improper payments and identify fraud

- Improve data analytics to reveal billing anomalies
- Improve investigations and audits to identify and recover improper payments
- Use administrative actions to sanction bad actors
- Streamline referral and investigation of suspected fraud

Personal care services in Medicaid managed care

- Implement parallel safeguards in managed care contracts

Prevention and deterrence activities protect beneficiaries and safeguard taxpayer funds

Prevention is the most effective way to protect Medicaid funds, but it is the *only* effective way to protect beneficiaries from harm. The traditional pay-and-chase strategy can, in principle, recover overpayment dollars, but harm to vulnerable beneficiaries can rarely be undone: because harm can and has included physical and emotional abuse and even death, harm can be irreversible. Consequently, vigorous prevention efforts must be paramount. Medicaid funds will benefit as well, because prevention measures aimed at improper payments are far more cost-effective than pay-and-chase methods for identifying and recovering improper payments.

The recommended mitigations advocated to address the vulnerabilities discussed under each of the strategic goals below are the result of the consensus reached by the diverse participant stakeholders at the MII course.

Ensure only screened and qualified providers oversee or provide care to beneficiaries

Because the personal care attendant spends extended periods of time alone with the beneficiary at home, usually without direct supervision, it is critical that attendants be thoroughly vetted through criminal background checks as well as trained and qualified to provide the services rendered. MII participants agreed that attendants should:

- Be screened and cleared of criminal conduct and citations for abuse by adult and child protective services agencies,
- Have their records continuously monitored for later criminal or abusive behavior,
- Be well-trained and qualified to provide the services rendered, and
- Be periodically re-trained to protect beneficiary welfare.

The risk to Medicaid funds in paying for services that are not directly supervised means that record keeping for accountability is also vulnerable to falsification. Unscrupulous providers are well positioned to take advantage of the vulnerabilities that persist in inadequate assessments, poor documentation, and lack of service specifications on claims. Fortunately, thorough screening through criminal background checks is also an effective preventive measure against dishonest billing.

Screening and Disclosures

The first step to minimizing risk to Medicaid beneficiaries and safeguarding funds from unscrupulous or abusive providers is to screen out these bad actors based on records of their past actions. Despite the critical importance of screening personal care providers, the most common type of error identified for personal support services in the 2016 PERM data was that providers had not been screened using risk based criteria when required.^{15,16}

¹⁵ Provider screening and enrollment requirements at 42 CFR Part 455, Subpart E.

¹⁶ CMS, [Medicaid and CHIP 2016 Improper Payments Report](#), November 2016.

Background Checks. MII participants and the HHS-OIG agree that states should employ independent background checks to ensure that personal care attendants as well as other PCS agency staff have clear histories according to standards established by the state.¹⁷ Several states require screening of attendants using criminal background checks (e.g., Alaska, Iowa, Minnesota, Nebraska, Ohio, Virginia, and the District of Columbia). CMS has awarded more than \$64 million to 26 states and territories to implement comprehensive background check programs for workers who apply for positions to provide direct resident or patient care.¹⁸

In addition to criminal background checks, MII participants recommended also screening against exclusion lists from Adult Protective Services (APS) and Child Protective Services (CPS) agencies. Some states have established centralized databases where different agencies can access the status of providers' background checks and/or history of excludable offenses (see [text box](#)).

Central background check database: Alaska has a background check program administered by the Division of Health Care Services, and provides access to related state agencies and licensing boards. The centralized database reduces cost and burden compared to keeping background check results isolated to individual agencies or counties.¹⁹

Employee Disqualification List: Missouri's Department of Health and Senior Services maintains an Employee Disqualification List of caregivers who have been disqualified due to beneficiary abuse, neglect, misappropriation of funds or property, or falsification of documentation. Provider agencies must check the Employee Disqualification List before employing caregivers.²⁰

PCS agencies or attendants that enroll in Medicaid as providers are subject to federal screening requirements. SMAs must require providers, as a condition of enrollment in Medicaid, to consent to Fingerprint-based Criminal Background Checks (FCBCs) according to 42 CFR 455.434 when required to do so under state law or by the level of screening based on fraud, waste, and abuse risk as determined for that category of provider in Medicare, if applicable. Because Medicare does not cover PCS, SMAs must assign Medicaid-only categories of providers such as PCS to an appropriate risk level.²¹ Note that Medicare has designated newly enrolling Home Health Agencies as a high-risk provider type, which requires FCBCs. Because of the similarities between home health services and PCS in caring for vulnerable beneficiaries in their homes, MII participants strongly recommended screening both attendants and PCS agency staff with FCBCs, as well as through APS and CPS exclusion lists.

¹⁷ Grimm, Christi A. (HHS-OIG), [Combating Waste, Fraud, and Abuse in Medicaid's Personal Care Services Program](#), Testimony before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, May 2, 2017.

¹⁸ [CMS National Background Check Program](#).

¹⁹ Alaska Division of Health Care Services, [Criminal Background Check Program](#).

²⁰ Missouri Department of Health and Senior Services, [Employee Disqualification List](#).

²¹ See "Risk Levels for Medicaid-Only Providers" in: CMS, [Medicaid Provider Enrollment Compendium](#) (MPEC), June 2017.

PCS can be provided in more than one service delivery model, including both agency-delivered services and self-directed services. Depending on each state's PCS program, self-direction flexibilities could convey to beneficiaries the ability to hire their own attendants. Care should be taken by SMAs and other state partners in the development of PCS parameters for self-direction to recognize that not all criminal histories carry the same risk of future misdeeds, and to recognize the role of the beneficiary in determining acceptable risk for background check issues.²²

Rap Back Service: For ongoing monitoring for any offenses committed by individuals after initial FCBC screening, states can implement Rap Back systems to automatically inform the SMA when new offenses occur. The SMA may then verify the new information and notify the employer, as appropriate.²³

Exclusion Registry Checks: In FFY 2015, Ohio used funding from the CMS National Background Check Program to implement a system that allows Medicaid providers to conduct screening of employees who provide direct care to the elderly and disabled populations. The system gives these Medicaid providers access to a Rap Back service and to a companion "Automated Registry Check System" (ARCS) to conduct pre- and post-hiring registry checks against the federal Excluded Parties List System (EPLS), the HHS-OIG's List of Excluded Individuals and Entities (LEIE), as well as Ohio's state databases for inmates, registered sex offenders, and abuser registries.²⁴

Disclosures. Providers who enroll in Medicaid are also required to submit disclosures of persons with ownership and control interest, any such persons with convictions related to government health care programs, and information related to certain business transactions on request, according to 42 CFR 455 Subpart B. Required disclosures provide valuable information that the SMA can use to screen providers for any significant financial relationships with disqualified individuals and cross-check with other sources for incorrect or undisclosed information that may reveal untrustworthy parties. These same regulations also provide the state with authorities to obtain disclosure of information related to certain business transactions which can reveal potential straw owners or other kickback relationships (§ 455.105) and to refuse or terminate a provider agreement if the provider did not fully and accurately disclose individuals with convictions related to government health care programs (§ 455.106). These disclosures must be updated within 35 days after any change in ownership as required by § 455.104, providing opportunities to carefully vet any new owners.

Site Visits. State Medicaid agencies must also conduct pre-enrollment and post-enrollment site visits of providers in the "moderate" or "high" risk categories, according to 42 CFR 455.432.

²² CMCS Informational Bulletin, [Strengthening Program Integrity in Medicaid Personal Care Services](#), December 13, 2016.

²³ Information on state Rap Back systems is available on the [CMS National Background Check Program's Technical Assistance website](#).

²⁴ Ohio Department of Medicaid, [Ohio National Background Check Program](#), November 2014.

The purposes of site visits are to verify the accuracy of disclosure information and to determine compliance with federal and state enrollment requirements. Thus, required site visits provide another method of checking for undisclosed parties or other information that may indicate that the provider does not meet the qualification standards set by the state, as permitted by 42 CFR 431.51(c)(2).

Provider Qualifications

Only qualified providers should be permitted to attend to the personal care needs of vulnerable beneficiaries in their homes, or to supervise attendants who provide care. MII participants agreed that minimum qualifications should be established for both attendants and PCS agency staff, while PCS agencies should be subject to credentialing standards and licensed by the state. Opinions varied as to whether standard qualifications should be established at the state or federal level. This mitigation has been advocated by the HHS-OIG, which continues to recommend that minimum qualification standards be established for PCS attendants.²⁵

Training. Initial as well as continuing education sanctioned by the state should be an integral part of oversight of PCS agencies. Training should include content essential for safe and effective care of the beneficiary (such as cardiopulmonary resuscitation (CPR), first aid, infection control, medication assistance, cleanliness); for providing care in a manner that comports with the beneficiary's personal, cultural, and/or religious preferences;²⁶ for accurate service documentation and billing; and for awareness of fraud, waste, abuse, and applicable whistleblower protections in state law. MII participants suggested that a state-approved online training program covering these topics would be a convenient method of including simple tests on content, warnings about responsibility for content, and maintenance of digital records of when identified individuals completed training. Compliance and good provider relations will be facilitated by helping PCS agency owners understand that effective training and compliance programs protect their profits by preventing situations that lead to overpayment recoveries, payment suspensions, or even termination.

Agency Financial Viability. PCS agencies may be more at risk of potential insolvency than most medical providers because there are few barriers to entry and the startup cost is more modest. The SMA may find that PCS agencies can accrue a balance of overpayments and go out of business before the state can recover the funds. Thus, to qualify for enrollment, PCS agencies should be required to provide evidence of financial viability or post surety bonds as a hedge against uncollectable overpayments. Alaska requires PCS providers to maintain financial records to show the provider's capacity to meet at least three months of operating expenses.²⁷ The District of Columbia requires PCS providers to post a surety bond of \$50,000 against all PCA services claims or legal judgments.²⁸

²⁵ Grimm, Christi A. (HHS-OIG), [Combating Waste, Fraud, and Abuse in Medicaid's Personal Care Services Program](#), Testimony before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, May 2, 2017.

²⁶ These best practices are required under the Community First Choice option. See: [77 FR 26828](#), § 441.565, May 7, 2012.

²⁷ [Medicaid coverage and payment for personal care services](#); Final filed regulations effective July 22, 2017; PCS Conditions of Participation (adopted by reference). The permanent link for these regulations will become available at: [Alaska Administrative Code: Title 7, Chapter 125, Article 1 – Personal Care Services](#).

²⁸ District of Columbia, [Medicaid Reimbursements for Personal Care Aide Services](#), Chapter 50 of Title 29, Public Welfare, of the D.C. Municipal Regulations, 63 DCR 14134 (§ 5011), November 18, 2016.

All parties—beneficiaries, providers, and the Medicaid program—benefit when providers understand fully the applicable Medicaid policy, their own responsibilities, and the penalties for noncompliance and improper billing. It is the Medicaid agency’s responsibility to provide clear policies and regulations, which may include providing policy communications for providers in other languages as needed. To confirm that providers recognize their responsibilities, MII participants recommended that SMAs require attestations in provider agreements that providers understand applicable SMA policies and regulations and acknowledge sanctions for noncompliance and penalties for fraud.

Registration and/or Enrollment

Final certification by the state that a provider has been screened and qualified to provide care to Medicaid beneficiaries serves as a critical gateway to minimize risk to both vulnerable beneficiaries and Medicaid funds. For PCS agencies, enrollment with the state serves this function, and it is critical that the information submitted for enrollment (screening, licensing, disclosures, and financial viability) be checked. MII participants emphasized that any percent change in agency ownership should require that a new screening and enrollment process be completed, along with checking new disclosures. States can set reasonable standards for provider qualifications using authority under 42 CFR 431.51(c)(2), and deny enrollment when standards are not met. In addition, states that wish to impose more frequent screening requirements upon prospective or enrolled providers may do so pursuant to § 455.452.

Caregiver Registry or Enrollment. Certification that personal care attendants have been screened and qualified by the state to provide care to Medicaid beneficiaries is perhaps the strongest recommendation from MII participants. Personal care attendants should be registered or enrolled with the state so that information about the identities, screening status, qualifications, training and re-training, and any offenses of all individual caregivers will be known to the SMA for tracking attendants over time (and when they move between agencies) and for tracking services on documentation and claims. The HHS-OIG continues to recommend strongly that CMS require states to enroll or register all PCS attendants and assign them unique numbers.^{29,30} CMS has solicited public input on whether and how states should be required to enroll or register all PCS attendants and assign them unique numbers for tracking claims, among related program integrity and other HCBS issues.³¹ Attendant registration can be accomplished through a state caregiver registry or a simplified enrollment process. Several states already enroll attendants in the Medicaid program (e.g., Alaska, Iowa, Minnesota, Nebraska, and North Dakota).

Attendant Identifiers. Assigning unique identifiers to PCAs is the most efficient way to identify the caregiver’s identity (as the rendering provider) on PCS claims submitted for payment and to facilitate tracking attendants’ transitions from place to place and/or from agency to agency. For these reasons, some states already assign state identifiers to attendants when they enroll with the

²⁹ OIG, [Personal Care Services: Trends, Vulnerabilities, and Recommendations for Improvement: A Portfolio](#), OIG-12-12-01, November 2012.

³⁰ Grimm, Christi A. (HHS-OIG), [Combating Waste, Fraud, and Abuse in Medicaid’s Personal Care Services Program](#), Testimony before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, May 2, 2017.

³¹ [81 FR 78760](#), November 9, 2016.

Medicaid agency (e.g., Alaska, Iowa, and Minnesota). The District of Columbia requires every Medicaid PCA to be certified as a Home Health Aide and to have an individual National Provider Identifier (NPI) number obtained from the National Plan and Provider Enumeration System (NPPES).³² CMS is determining the feasibility of allowing states to use NPIs to enumerate Medicaid caregivers as Personal Care Attendants to support their program integrity efforts.³³ MII participants favored allowing states to use an individual national identifier such as the NPI for attendants because doing so would avoid the expense to states of setting up their own system of unique identifiers for PCAs and would facilitate tracking of bad actors across state lines.

The SMA's gatekeeping function of allowing only screened and qualified providers and attendants to provide care to Medicaid beneficiaries while denying questionable or unqualified individuals from gaining access to both Medicaid beneficiaries and funds is the single most effective strategy of prevention available. Such work should be conducted with considerable care and attention, and staff who process enrollment applications and check submitted information should understand that their work serves a critical program integrity function. Their care in performing enrollment work and accurately recording information in the Medicaid Management Information System (MMIS) provider databases or in caregiver registries can prevent a beneficiary from suffering harm and can avoid losing Medicaid dollars to fraudsters.

Risk: Harm to beneficiaries and loss of Medicaid funds from unscrupulous providers

Vulnerabilities

Unscreened or Unqualified Providers

- Attendants who are not screened or qualified working with beneficiaries alone at home, exposing beneficiaries to risks of harm from substandard services, theft, neglect, or abuse.
- Risk of loss of Medicaid funds through fraud, waste, or abuse committed by unscreened or incompletely screened providers—e.g., through kickbacks and other forms of collusion to falsify assessments or timesheets to obtain improper payments.
- PCS agencies enrolling with owners or managers who lack appropriate qualifications for operating a PCS agency.
- PCS agencies being only “registered” as businesses and not licensed as qualified PCS agencies.

Noncompliant Providers

- Inadequate provider requirements that allow enrollment of providers with questionable backgrounds or qualifications, and allow previously terminated providers to re-enroll despite their history of sanctions.

³² District of Columbia, [Medicaid Reimbursements for Personal Care Aide Services](#), Chapter 50 of Title 29, Public Welfare, of the D.C. Municipal Regulations, 63 DCR 14134 (§ 5009), November 18, 2016.

³³ The taxonomy code “Personal Care Attendant” (3747P1801X) designates an individual who provides assistance with eating, bathing, dressing, personal hygiene, and activities of daily living as specified in the plan of care. The Healthcare Provider Taxonomy Code Set is available from the [Washington Publishing Company](#).

- Lack of caregiver identifiers make it possible for offenders to move from place to place or agency to agency.
- Noncompliant providers gaining concessions in appeals judgments or lessened sanctions after claiming not to have understood Medicaid policy or penalties for noncompliance.
- Changes in PCS agency ownership may introduce disqualified individuals, which could place the SMA at risk for payments made to PCS agencies that fail to disclose changes in ownership or control information as required by 42 CFR 455.104.

Background Checks

- Lack of funding to implement background checks or lack of requirement that PCS agencies provide independent background checks for all attendants.
- Results of background checks not being carefully reviewed and cleared, or even faked, especially when delegated to PCS agencies.
- Criminal background checks do not extend to screening against exclusion lists from adult or child protective services (APS or CPS).
- Providers who clear background checks initially, but who later commit criminal, APS, or CPS offenses that put beneficiaries at risk.
- Lack of a central database where different state agencies can access the status of providers' background checks. Background check results that are not shared from county to county.
- Completion of agency enrollment without a cleared background check. Allowing attendants to work with incomplete background check clearance. Failure to follow up on completing background checks for attendants allowed to work on provisional approval.

Lack of transparency about providers

- Medicaid agencies lack information about the identities of caregivers who work for agencies, and therefore lack information about caregivers' training, qualifications, or background screening status. When investigating fraud allegations, contacting the PCS agency to acquire this information discloses the existence of an investigation to the agency.
- Providers with incomplete screening or substandard qualifications.
- Inaccurate or Incomplete Disclosures: PCS agency owners who fail to disclose disqualifying information (e.g., straw PCS agency ownership, where true owner may be on federal exclusion list). Collusion between owners and managers in hiding information. Difficulty in obtaining accurate corroborating information on PCS agency owners.
- PCS agencies with weak financial viability can accrue a Medicaid credit balance and go out of business before the state can net the credit balance against future claims, resulting in loss of overpayments to the state and potential interruption of services to beneficiaries.

Mitigations

Background Checks

- Implement a comprehensive fingerprint-based criminal background check program for screening PCS agency staff, attendants, and new applicants for employment.
- Use an independent agent to conduct, carefully review, and clear fingerprint-based criminal background checks of PCS agency staff and attendants. Check applicants against APS and CPS exclusion lists.
- Establish a central database where different agencies can access the status of providers' background checks and/or history of excludable offenses (see [previous text box](#)).
- Monitor provisional approvals for attendants to work with incomplete screening to confirm that background checks are completed, reviewed, and cleared timely. Where variances are granted for attendants with background check issues, implement closer monitoring/supervision.
- For ongoing monitoring to detect any future offenses, use a Rap Back service to promptly detect any new criminal offenses (see [previous text box](#)), and re-check APS and CPS exclusion lists to detect any other confirmed offenses, especially by attendants.

Provider Qualifications

- Establish state regulation to require PCS agencies to be licensed by the state licensing board, with required minimum qualifications and standards for credentialing and periodic re-credentialing.
- Establish minimum qualifications for attendants, including requirements for continuing education.
- Require PCS agencies to demonstrate proof of financial viability at enrollment and/or require surety bonds to cover future overpayments and unpaid attendant wages in the event of agency failure.

Provider Training

- Clarify policies and regulations, and provide clear guidance materials for providers on their responsibilities and on penalties for noncompliance.
- Establish compliance programs for PCS agencies: require substantive, state-approved training (including training on fraud, waste, abuse, and applicable whistleblower protections) for staff in all roles across the PCS provider spectrum—agencies, attendants, and attendants in self-directed care.
- Required training should include signatures attesting to attendance, responsibility for content, and acknowledgement of penalties for noncompliance. Maintain accurate records of training along with attestations, which are needed to support successful prosecutions.
- Include examples of fraud, improper payment detection, and prosecution during training and in provider attestation forms.
- Require annual continuing education for agencies. Require agencies to conduct periodic in-service training for attendants.

- Conduct remedial training as part of a corrective action plan for noncompliant providers to mitigate against future legal defense arguments that continued noncompliance was due to ignorance or administrative error. Maintain records of provider's attestations of attendance and responsibility for content.

*PCS Agency Enrollment*³⁴

- Require attestations in provider agreements that providers understand policy and contract requirements and acknowledge sanctions for noncompliance and penalties for fraud.
- Require new screening and enrollment for any changes in agency ownership.
- Disclosures: Cross-check disclosures of ownership and control with other sources to reveal any undisclosed owners that would make the provider ineligible for enrollment. Remind agencies to update disclosures within 35 days after any change in ownership as required by 42 CFR 455.104.
- Conduct pre-enrollment and post-enrollment site visits to check disclosure information and determine compliance with applicable requirements. Follow up with unannounced on-site inspections, especially for providers with compliance issues. (42 CFR 455.432)
- Refuse or terminate a provider agreement if the provider did not fully and accurately disclose individuals with government health care convictions, using authority under 42 CFR 455.106.
- Strengthen state standards for provider qualifications, consistent with the limitations in 42 CFR 431.51. Deny enrollment when standards are not met.

Attendant Registration or Enrollment

- Establish a caregiver registry or simplified enrollment to track attendants' screening results, qualifications, training and re-training, certifications, and any confirmed offenses.
- Assign a unique identifier to each attendant to facilitate tracking the attendant's work on documentation of service records and as the rendering provider on claims. Require each PCA to affiliate with a PCS agency to clarify the PCA's employer, and implement an MMIS edit to prevent payment of claims where the billing and rendering providers are not affiliated.
- Require attestations that attendants understand their contract requirements and the Medicaid policy applicable to their duties, and acknowledge sanctions for noncompliance and penalties for fraud, waste, and abuse.
- To prevent offending caregivers from moving from agency to agency, require PCS agencies to report caregiver terminations for cause, including professional incompetence and unprofessional or unethical conduct (e.g., submitting timesheets for services not rendered).

³⁴ For Mitigations regarding previously terminated providers re-applying for enrollment, see section on [Administrative Actions](#).

Approve eligible beneficiaries for services appropriate to their needs

Personal Care Services often require daily care to beneficiaries, resulting in regular recurring costs to the Medicaid program. Thus, recurring payments for unneeded services can occur due to vulnerabilities in determination of beneficiary eligibility, in assessment of beneficiary needs for PCS, and in authorization of services. PCS agency staff who assess the need for services could have a conflict of interest because their agency will benefit financially from more clients receiving more services. Likewise, state staff authorizing more services than determined necessary by a functional needs assessment leads to recurrent wasteful spending. The precedents set by inadequate authorizations can lead to further waste of state resources when implementation of appropriate authorization criteria leads to time-consuming appeals of denials or of reductions in services. Nevertheless, we have a responsibility to ensure that services that are needed are provided to eligible beneficiaries at the appropriate frequency and quality.

The balance of approving needed services for one beneficiary while preventing payment for unneeded or excessive services for another beneficiary requires a carefully designed and implemented program of functional assessment of beneficiaries' needs for services.

Risk: *Payment for unneeded services*

Vulnerabilities

- Conflict of interest when PCS agencies (or those with shared interests) conduct assessments.
- Service authorizations and/or plans of care that call for more services than needed.
- Some providers and/or beneficiaries may collude to obtain authorization for services not needed or for a higher level of services than needed, which may involve coaching beneficiaries on how to feign or exaggerate disabilities.
- Inadequate assessment or authorization practices leading to approval of unneeded (including higher than needed) services. High caseloads and the extra work to justify and subsequently defend denials can lower the threshold for approval.
- Beneficiary or family member purposefully exaggerating initial needs, or feigning continued need when medical condition improves.
- Unneeded services may be approved by individuals not trained in functional needs assessment—e.g., case managers or physicians.

Mitigations

- Both initial functional needs assessments and reassessments should be conducted face-to-face by *qualified independent agents* using *validated assessment tools* in consultation with the individual and the individual's identified supports, consistent with federal regulations.³⁵

³⁵ CMS published a HCBS final rule ([79 FR 2948](#), January 16, 2014) including provisions regarding assessment and reassessment of functional need by an independent and qualified agent, as well as conflict of interest standards. (See, for example, 42 CFR §§ 441.720, 441.730.)

- Assessment policy should include criteria for determining the frequency of reassessments and a provision that the state can conduct reassessments at its discretion to prevent waste in cases where a previous level of services is no longer needed because of significant improvement in the beneficiary's condition.
- Implement quality control checks of assessments. Review care plans before authorization. Conduct follow-up visits to detect fraud and to ensure beneficiaries are receiving the services described in their care plan.
- Ongoing training for assessment personnel should include program integrity vulnerabilities and mitigations.
- Education for beneficiaries should include the importance of honest representation of needs, fraud awareness, and how to report fraud.

Qualification Steps for Personal Care Services

The District of Columbia Department of Health Care Finance (DHCF) requires the following steps for PCS to be provided to a Medicaid beneficiary:

- 1) A Medicaid-enrolled physician or Advanced Practice Registered Nurse (APRN) examines the beneficiary and provides a written order that certifies that the beneficiary is unable to perform one or more ADL for which PCS are needed.
- 2) The DHCF or its designee conducts an independent face-to-face assessment using a standardized assessment tool to evaluate the beneficiary's need for assistance with ADL.³⁶
- 3) Based on that assessment, the DHCF issues a service authorization that specifies the amount, frequency, duration, and scope of PCS authorized to be provided to the beneficiary.
- 4) The DHCF makes a referral to the beneficiary's choice of a qualified PCS agency, which employs a Registered Nurse to develop a plan of care in consultation with the beneficiary and the family or authorized representative, consistent with the needs assessment and service authorization.
- 5) The plan of care must be approved and signed by the beneficiary's physician or APRN within thirty (30) days of the start of care.³⁷

³⁶ District of Columbia, [Long Term Care Assessment Tool](#), November 2015.

³⁷ District of Columbia, [Medicaid Reimbursements for Personal Care Aide Services](#), Chapter 50 of Title 29, Public Welfare, of the D.C. Municipal Regulations, 63 DCR 14134 (§ 5002–§ 5006), November 18, 2016.

Ensure services are fully and accurately documented

Vulnerabilities in documentation requirements can prevent Medicaid agencies from detecting that beneficiaries are not receiving the authorized services they need, and can defeat opportunities to use one of the most effective methods of preventing future improper payments to enrolled providers—termination of fraudulent providers from the Medicaid program. For fraud investigations of billing for services not provided, missing attendant identity and/or missing service start and stop times prevent investigators from determining whether the attendant was located elsewhere at the times during which services were supposedly being performed. The ability to prosecute and terminate the participation of unscrupulous providers from the Medicaid program depends critically on having specific details regarding the claimed services to demonstrate the falsification of claims. Lack of documentation means lack of potential evidence in cases of fraudulent claiming. When documentation requirements are not enforced, unscrupulous providers are able to continue denying needed services to beneficiaries and misdirecting Medicaid funds to enrich themselves at taxpayer expense.

Documentation requirements generally include plans of care, documentation of services provided, and timesheets showing start and stop times to support the amount of services billed. PCS documentation requirements exist to check that beneficiaries receive services in accordance with approved plans of care; that caregivers provide the type, amount, and frequency of services consistent with beneficiaries' approved plans of care; and that claims for payment are supported by records that verify that all billed services were actually provided. In the 2016 PERM report, most of the errors identified in medical review for claims in the category of personal support services (which include PCS and other services) were incomplete documentation errors due to missing active plans of care, missing notes verifying receipt of services, missing daily documentation of specific tasks, and missing or incorrectly documented numbers of units of service. In addition, PERM identified personal support services as the most common provider type cited for failing to provide any documentation to support their Medicaid claims.³⁸

Documentation should provide sufficient details to allow reviewers and investigators to validate that services were actually provided in accordance with Medicaid policies, and include signatures attesting to the accuracy of the record. Implementing a service verification system for attendants to itemize tasks performed and enter their start and stop times establishes the clear expectation that attendants are held accountable for time billed, provides the specific documentation needed to substantiate that services were performed, and can provide the opportunity to detect attempts to obtain payment for services not authorized.

To ensure that beneficiaries actually receive the correct services indicated in their plans of care and reflected in billed claims, requirements for maintaining documentation and procedures for periodic review of documentation should be improved.

³⁸ CMS, [Medicaid and CHIP 2016 Improper Payments Report](#), November 2016.

Risk: *Payment for services lacking valid or adequate documentation*

Vulnerabilities

- Claims paid without adequate supporting documentation, including in consumer-directed PCS.
- Providers may coerce or collude with beneficiaries to sign false or blank timesheets, sharing proceeds of payments for services not rendered as an inducement to collusion.
- Poor compatibility between service timekeeping records and MMIS makes it difficult to verify billed services.
- Bundled billing by fiscal intermediaries for aggregated services provided to many beneficiaries over many days provides poor transparency to individual services, particularly in self-directed care.
- Lack of documentation regarding who rendered services, amount of services, or start and stop times can hamper prosecution. Visit verification systems often lack details of service tasks rendered.
- Electronic timesheets often lack a requirement for a confirming signature by the beneficiary or a representative.

Mitigations

- Establish standard requirements for sufficiently detailed documentation of care plans; for service logs with attendants identified, start/end times, and tasks performed; and for supervisory visits.
- Educate providers that compliant documentation protects their income from overpayment recapture. Conduct spot checks of documentation, and repeat as needed for noncompliant providers.
- Implement Electronic Visit Verification (EVV) to provide meaningful information for program integrity purposes: require the EVV vendor to produce monthly reports of service data in a specified format to facilitate compatibility with MMIS.³⁹
- Develop a database for service verification data that can be cross-checked with service details extracted from claims data. Develop and run queries on a regular basis to identify discrepancies. Investigate significant, repeated anomalies.
- Improve support systems in self-directed care to clarify guidance and provide training on proper documentation procedures.
- Educate beneficiaries as well as providers about types of PCS fraud (e.g., collusion, signing timecards for services not rendered) and resulting penalties.
- Include honesty affirmations for all signatures on timesheets. Where electronic timekeeping systems lack a provision for signatures, require agencies to maintain paper backup of timesheets with beneficiary signatures.

³⁹ Section 12006 of the [21st Century Cures Act](#) (Public Law 114–255) requires states to implement an EVV system for Medicaid PCS by January 1, 2019.

Require claims to include complete specifications regarding services

Claims that providers submit for payment are the attested record of the services that providers claim to have rendered, and are thus the record of services that the SMA relies upon to validate whether payment should be made. If claims information can be demonstrated to be intentionally falsified to obtain payment for services not rendered, the fraudulent providers can be removed from the Medicaid program, prosecuted, excluded from participation in Medicare and other states' Medicaid programs, and prevented from continuing to commit fraud.

However, claims that lack sufficient detail regarding the billed services often cannot provide the evidence needed to prove fraudulent billing. For example, if investigators have reason to suspect that an attendant was working another job during hours when their services were billed for PCS, absence of claim information regarding the identity of the attendant or the units of service billed for each date of service can be an impediment to proving fraud. To mitigate these types of vulnerabilities, the HHS-OIG continues to recommend strongly that PCS claims identify the specific dates of service and the PCS attendant who provided the service.^{40,41} Supporting documentation such as timesheets discussed in the last section provide one potential source of evidence of fraud, but timesheets are not available in MMIS to validate against other claims or against other relevant data. In addition, requiring both the claim and the supporting documentation to show the identity of the attendant and the units of service provided for each date of service provides the opportunity to detect a fraudulent mismatch between claims and supporting documentation. Minnesota implemented a requirement in 2009 for PCS claims to bill for each date of service on a separate claim line with the identity of the individual PCA as the rendering provider on each claim line.⁴² Alaska, the District of Columbia, and Iowa (in Consumer Directed Attendant Care) also require attendant identifiers on PCS claims.

Furthermore, availability of claim details about who rendered how many units of service on which dates provides a richer substrate of MMIS data available for automated prepayment review (e.g., to detect PCS billed during hospital stays). Additionally, these claim details may be used for post-payment data mining algorithms to search across a large number of claims from many providers to identify outliers as potential audit targets (e.g., attendants working a suspiciously large number of hours over a period of time). The practice of paying claims billed over a range of dates for aggregated units of service defeats many of the methods that data analysts can use to detect potential improper payments.

Because claims that providers submit for payment are the SMA's most important record of the services that providers claim to have rendered, improvements are needed in specifying service details more completely.

⁴⁰ OIG, [Personal Care Services: Trends, Vulnerabilities, and Recommendations for Improvement: A Portfolio](#), OIG-12-12-01, November 2012.

⁴¹ Grimm, Christi A. (HHS-OIG), [Combating Waste, Fraud, and Abuse in Medicaid's Personal Care Services Program](#), Testimony before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, May 2, 2017.

⁴² Minnesota Department of Human Services, [Personal Care Assistance Services](#), "Billing: Submitting PCA Claims," revised March 2015.

Risk: *Payment for services not provided due to insufficient details on claims*

Vulnerabilities

- Absence of attendant identifiers on claims prevents opportunities to use this information to check whether the attendant had been cleared to provide PCS or to detect improper payments through prepayment review or data mining (e.g., same attendant providing overlapping services), or through post-payment audits and investigations (e.g., attendant located elsewhere).
- Billing for services not provided: billing for services while attendant is not working, working at another location, attending school full-time, on vacation, or beneficiary is in the hospital or visiting elsewhere.
- Billing over a range of dates obscures the dates on which services were actually provided as well as how many units of service are billed for each date of service, preventing opportunities to use this information to detect conflicts involving individual dates of service through prepayment review, data mining, or post-payment audits and investigations.
- “Faucet payment” systems that make payments on a monthly or quarterly basis with no itemized billing and inadequate requirements for service logs.

Mitigations

- Require claims to specify units of service for each date of service on separate claim details.
- Require claims to include an attendant identifier as the rendering provider on all claim details.

Optimize prepayment review to prevent improper payments

The use of automated prepayment edits and audits⁴³ in the MMIS claims processing system can be a very powerful method for preventing improper payments when interfaced with complete and accurate data from other available sources. Claims can be automatically checked to confirm that providers have been properly screened and enrolled or registered; that beneficiaries are eligible for services; and that services have been authorized for the type, amount, and frequency of services billed. Claims can also be automatically checked for conflicts with other claims (e.g., PCS billed during hospital stays) and for third party liability. Ideally, interfacing MMIS with EVV systems would enable automatically cross-checking billed claims against submitted timesheets for any discrepancies.

While the MMIS could perform all these automated checks, the system cannot do so effectively if claims are not required to include sufficiently specific information such as the identity of attendants and the quantity of services billed for each date of service, as detailed in the previous section. MMIS claims adjudication processes are also limited in their ability to validate claims

⁴³ *Edits* verify that the claim contains valid data—e.g., that the provider number is legitimate. *Audits* check whether the service being billed has certain policy restrictions based on other services in claims history (e.g., once-in-a-lifetime procedures such as appendectomy being billed again).

by the accuracy and completeness of data tables containing relevant information. For example, if relevant data tables do not accurately indicate whether the service has been authorized for the beneficiary or whether providers have completed all screening and enrollment or registration requirements, then payment cannot be blocked for these types of improper claims.

To maximize the power of automated claims validation by the MMIS to prevent improper payments, improvements are needed in expansion of prepayment edits and audits to cross-check against other available data, and in the accuracy of data tables containing beneficiary eligibility for PCS (assessment outcomes), service authorizations, and provider enrollment or registration status.

Risk: Paying claims with detectable data conflicts

Vulnerabilities

- Payment for services not authorized, in excess of amount authorized, or that should *not* have been authorized because of failure to link independent assessment of needs to authorization of services.
- Payment for overlapping services; payment for PCS during an institutional stay (except for authorized retention payments).
- Payment for billers with incomplete enrollment (incomplete screening, qualifications, or disclosures) or for services by unscreened or uncertified attendants.
- Billing for unreasonable units of service over a span of time.

Mitigations

- Use prepayment review to block payment for services not authorized. Check that services authorized accurately reflect independent needs assessments.
- Supplement MMIS claims processing prior to making payment by using a contractor to conduct more extensive prepayment review.
- Establish daily caps corresponding to maximum reasonable quantity of services for a single attendant and/or a single beneficiary, and implement prepayment edits to pend or deny claims that exceed caps.
- Implement processes to cross-check accurate screening and qualification status for all active providers in MMIS data tables. Confirm that edits are actively implemented to block payment for billers with incomplete enrollment (incomplete screening, qualifications, or disclosures) or for services by unscreened or uncertified attendants.
- Improve prepayment review for PCS, including prepayment audits to block payment for PCS during an institutional stay, except for authorized retention payments.
- Fully implement National Correct Coding Initiative (NCCI) edits for PCS to prevent payment for overlapping or mutually exclusive procedures.

Post-payment review can recover improper payments and identify fraud

Identifying potential overpayments through data mining, and confirming and recovering overpayments through audits, remain valuable tools in combatting Medicaid fraud, waste, and abuse. As discussed in the above sections, requiring more detailed service data on claims (attendant identity; units of service on each date of service) and implementing methods for cross-checking service verification data with MMIS claims will provide a richer substrate of data available for post-payment review to use in detection of potential overpayments. Likewise, the same richer data set will provide investigators with more avenues for proving and prosecuting fraud.

Improper payments due to fraud, as undesirable as they are, provide opportunities to terminate fraudulent providers from the Medicaid program. In cases where fraud is suspected but not yet proven, State Medicaid Agencies can use their authority to temporarily suspend all Medicaid payments to a provider after the agency determines there is a credible allegation of fraud for which an investigation is pending.⁴⁴ Payment suspensions can stop the flow of likely improper payments while the MFCU is investigating whether or not the fraud allegation is confirmed. If confirmed, the fraudulent provider can be terminated from the Medicaid program, prosecuted, and improper payments recovered along with any monetary penalties.

Thus, a strong program of detection, audit/investigation, and administrative action is key to preventing future improper payments by terminating fraudulent providers. Viewed in this context, fraud investigations and the supporting data analytics and audits can be viewed as important parts of an effective program of prevention of future improper payments.

Improve data analytics to reveal billing anomalies

Given sufficient service details on claims and relevant information available in databases containing accurate provider and beneficiary information, data analysts can develop algorithms to detect a wide variety of anomalous patterns that indicate potential overpayments, including those due to fraud, waste, or abuse.

Any conflict or irregularity that could have been detected with prepayment edits/audits can be identified with post-payment algorithm runs in circumstances where prepayment edits/audits are not yet implemented or were temporarily turned off. Regularly running algorithms that imitate prepayment edits/audits as a backup for prepayment review can compensate for vulnerabilities due to inactive edits/audits and for later additions to claims history. For example, when hospitals bill later than PCS agencies, prepayment review is unable to detect PCS billed during hospital stays because the PCS claim is paid before the hospital claim is submitted—a conflict that a periodic post-payment algorithm run can easily detect.

Post-payment data analytics can also help to identify other vulnerabilities in prepayment review processes, such as when claims edits do not accurately cross-check claims with provider enrollment data or limits set in service authorizations. Performing such algorithm runs can demonstrate the cost savings that would be achieved by implementing the corresponding

⁴⁴ 42 CFR 455.23. Final rule CMS-6028-FC, [76 FR 5862](#), February 2, 2011.

prepayment edit/audit to support assigning an appropriate priority for the necessary MMIS change request to implement an edit/audit in prepayment claim adjudication.

Data analysis can also detect patterns of anomalous billing without algorithms targeted to specific schemes. For example, reviewing quarterly utilization patterns across PCS providers and beneficiaries, calculating statistics such as hours billed per PCA, and examining outliers can reveal potential audit targets. If only one or two PCS agencies are billing the maximum number of hours for all of their PCAs with no variation while most agencies are not, a review of documentation for the outlier agencies may be in order.

***Risk:** Improper billing not detected by prepayment review*

Vulnerabilities

- Prepayment review systems that fail to block payment for services not authorized or in excess of amount authorized.
- Prepayment review systems that fail to block payment for overlapping services.
- Improper payments for PCS during an institutional stay (except for authorized retention payments) which were not blocked by prepayment review due to hospital billing after PCS claim was paid, as well as other improper payments that cannot be detected by prepayment review.
- Prepayment review systems that fail to block payment for billers with incomplete enrollment (incomplete screening, qualifications, or disclosures) or for services by uncertified attendants.
- Loss of potential cost savings from unimplemented prepayment review because of delays resulting from long turnaround for MMIS change requests, contract renewals, or delays in implementing a new system.
- Improper payments made due to temporarily inactivating prepayment edits or audits.
- Payments made for billing unreasonable units of service over a span of time.
- Improper payments made due to lack of an implemented method for cross-checking service verification data with MMIS claims.
- Absence of attendant identifiers and individual dates of service on claims prevents data mining from detecting claims for overlapping or geographically improbable services by the same attendant, and also prevents investigators and prosecutors from having evidence of fraud for billing services when the attendant was elsewhere.

Mitigations

- Run algorithms to detect improper payments resulting from unimplemented or inactivated prepayment edits/audits (e.g., duplicate services, PCS overlapping institutional stays, incompletely enrolled billers, services by uncertified attendants, units of service exceeding caps) and other billing anomalies.
- Instruct the MMIS contractor to notify post-payment analysts when specific prepayment edits/audits are temporarily inactivated for a specified period so that data analysts can

periodically run algorithms to detect claims that prepayment edits/audits would have identified, and take appropriate action.

- Demonstrate cost savings that would be achieved by implementing specific prepayment edits/audits by performing post-payment algorithm runs that imitate the function of the proposed edit or audit. Compare the cost of staff time in conducting post-payment analysis, audits, and overpayment recovery to the cost of implementing the corresponding automated prepayment edits/audits. Use this information to support assigning an appropriate priority for the necessary MMIS change request to implement an edit/audit in prepayment claim adjudication.
- Conduct post-payment data analysis to cross-check service verification data with MMIS claims to detect documentation mismatches and make recommendations for follow-up audits.
- Periodically run algorithms to detect when individuals are both providing and receiving services to detect any anomalies.
- Review quarterly utilization patterns across PCS providers and beneficiaries, calculating statistics such as hours billed per PCA, and examine outliers to identify potential audit targets.
- Improve the use of available external data sources to allow earlier detection of cases where claims should not be paid—e.g., new offenses by providers ([Rap Back service](#)), deceased individuals (Social Security Administration’s Death Master File (DMF)),⁴⁵ incarceration and court records, employment records, Medicare’s Provider Enrollment Chain and Ownership System (PECOS), and beneficiaries crossing state lines (Public Assistance Reporting Information System (PARIS)).

Improve investigations and audits to identify and recover improper payments

Audits and investigations of potential improper payments provide the definitive evidence with which overpayments are recovered, settlements or prosecutions are finalized, and fraudulent providers are terminated from the Medicaid program. Promising targets identified through data analytic methods discussed in the preceding section can be audited to determine whether the provider has maintained documentation that services were provided in accordance with the approved plan of care, and are complete and accurate—e.g., signed timesheets showing start and stop times to support the amount of services billed. One advantage of auditing PCS is that because PCAs are typically not licensed medical professionals, non-medical staff can be trained to audit timesheets and service logs of tasks performed to check that the documentation corresponds to services authorized and claims paid. Medical reviewers can focus on auditing care plans when necessary to check that they accurately and completely reflect the independent functional needs assessment.

⁴⁵ As of May 2017, CMS has made DMF data available to pilot states via TIBCO, the file server where states currently also access PECOS provider file extracts, Medicare revocations, Medicaid terminations, and OIG sanctions.

Audit Contractors. To accomplish more oversight and monitoring of PCS providers without increasing the demand on limited state resources, states can use contractors to extend staff resources for undertaking PCS audits. The cost of audits by contractors may be lower due to review of timekeeping records by non-medical staff, but SMAs should still be mindful of provider burden and sufficient return on investment. In addition, states have the opportunity to work with CMS to undertake collaborative audits with federal audit contractors to audit PCS claims without spending state funds.⁴⁶

Probe-and-Educate Strategy. Most providers are not fraudulent, but rather operate on a continuum of noncompliance from unintentional billing errors, to limited errors on specific issues, to significant patterns of abuse on multiple issues without progressing to outright fraud. Audits provide an opportunity to identify specific issues with provider billing, recover overpayments, and provide focused education to the provider based on the identified audit findings. PERM reports have consistently found that missing or incomplete documentation errors are among the most common root causes of improper PCS payments, with personal support services as the most common category of providers cited for providing no documentation to support their Medicaid claims.⁴⁷ For any service type with widespread low-level compliance failures where the goal is primarily provider education, reviewers can sample a very small number of claims for each provider, identify specific billing and/or documentation issues, and provide focused education—referred to as a “probe-and-educate” strategy.⁴⁸ CMS provides provider education toolkits on the *Medicaid Program Integrity Education* website, including toolkits targeted to increasing provider awareness of documentation requirements and other issues in PCS program integrity.⁴⁹

Whether audits and investigations identify and recover overpayments, lead to improved provider compliance through a probe-and-educate strategy or sentinel effect,⁵⁰ or provide evidence of fraud to convict and terminate fraudulent providers, post-payment reviews are an important part of the state’s Medicaid program integrity strategy and contribute significantly to prevention of future improper payments.

Risk: Improper payments due to fraud, waste, and abuse

Vulnerabilities

- Paid claims that lack adequate supporting documentation (care plans, authorizations, service logs), including in consumer-directed PCS.

⁴⁶ CMS began transitioning the work of the Audit Medicaid Integrity Contractors (MICs) to Unified Program Integrity Contractors (UPICs) in FFY 2017 to better coordinate Medicare and Medicaid program integrity audit and investigation work.

⁴⁷ CMS, [Medicaid and CHIP 2016 Improper Payments Report](#), November 2016.

⁴⁸ CMS, [Selecting Home Health Claims for Probe and Educate Review: Episodes that Begin on or After August 1, 2015](#), MLN Matters # SE1524, November 9, 2015.

⁴⁹ CMS, [Medicaid Program Integrity Education](#), updated November 2017.

⁵⁰ Applied to provider compliance, the sentinel effect is the tendency for compliance to improve across the peer group after providers observe examples of evaluation and enforcement actions such as audits, investigations, prosecutions, or convictions.

- Payment for services not provided, or provided by incompletely screened attendants or agencies with enrollment anomalies (excluded parties, or incomplete or fraudulent disclosures).
- Prepayment review systems that fail to block improper payments (as detailed in the previous section for data analytic vulnerabilities).
- Improper payments made due to absence of claim information regarding the identity of the attendant or the units of service billed for each date of service.

Mitigations

- Based on results of data analytics, audit cases of suspicious billing by comparing claims to service logs and reviewing documentation for required authorizations and approved plans of care.
- Strengthen investigative capabilities by nurturing strong interagency relationships to share data that can reveal fraudulent activity (e.g., attendant or beneficiary employed or present elsewhere during claimed service periods).
 - If a PCA is suspected to be working elsewhere or attending classes during times when their services were billed, check state employment records or nearby enrollment records as appropriate.
 - If a PCA is suspected to be traveling out of the country during times when their services were billed, contact the Department of Homeland Security for records of international travel.
- State staff can use social media to check on outside activities for detecting suspected absences of attendant or beneficiary during claimed service periods.
- Work with the state's and/or CMS's audit contractors to audit PCS providers.
- Improve provider compliance with documentation and billing requirements by using a “probe-and-educate” strategy—auditing a small sample of claims and providing focused provider education tailored to each provider's compliance issues.
- Disseminate PCS provider education using CMS's HCBS/PCS provider education toolkits on the *Medicaid Program Integrity Education* website.⁵¹
- Use authority to obtain disclosure of information related to business transactions to reveal potential straw owners or other kickback relationships.⁵² Conduct unannounced on-site inspections for providers under investigation using authority under 42 CFR 455.432(b) to check for undisclosed information or noncompliance that may indicate that the provider does not meet the qualification standards set by the state.

⁵¹ CMS, [Medicaid Program Integrity Education](#), updated November 2017.

⁵² CMS, [Toolkits to Address Frequent Findings: 42 CFR 455.105 Disclosures of Business Transactions](#), December 2014.

Use administrative actions to sanction bad actors

Payment Suspension. States have a powerful tool to withhold payments in cases where fraud is suspected but not yet proven: CMS published a final rule in 2011 that requires State Medicaid Agencies to temporarily suspend all Medicaid payments to a provider after an agency determines there is a credible allegation of fraud for which an investigation is pending, absent good cause not to suspend.⁵³ Thus, judicious use of payment suspensions can stop the flow of likely improper payments while the MFCU is investigating whether or not fraud has occurred. CMS has published a toolkit to assist states with the proper use of their payment suspension authority.⁵⁴

Termination. The most effective method of preventing fraudulent providers from obtaining future improper payments is to terminate such providers from the Medicaid program. Given sufficient evidence of recalcitrant noncompliance and/or fraud, SMAs can terminate providers for cause in accordance with their state regulations, and MFCUs can prosecute fraudulent providers.

Some MII participants reported that any willing provider laws in their states resulted in terminated providers later re-enrolling if they did not have convictions that required exclusion from government health care programs by the HHS-OIG. However, federal regulations allow states to set reasonable standards relating to the qualifications of providers,⁵⁵ and provide authority to refuse or terminate a provider agreement if the provider did not fully and accurately disclose the identities of persons with ownership or control interest, agents or managing employees, or persons with government health care convictions.⁵⁶ Some states can terminate or decline enrollment of a provider because doing so is judged to be in the best interests of the state's Medicaid program (see [text box](#)).

“Best Interest” Authority to Deny or Terminate Provider Enrollment

The Ohio Administrative Code gives the Medicaid Director “best interest” authority to deny or terminate a provider agreement if it is not in the best interest of Medicaid recipients and/or the State of Ohio.

Ohio's regulation describing this authority, “Termination and Denial of Provider Agreement,” lists many circumstances under which the Medicaid Director's “best interest” authority may be exercised—e.g., failing to cooperate or provide records or documentation upon request during an audit or review of provider activity; prescribing, authorizing, or billing for services that are not medically necessary; or failing to repay an overpayment assessed as a result of a final adjudication order.⁵⁷

⁵³ 42 CFR 455.23. Final rule CMS–6028–FC, [76 FR 5862](#), February 2, 2011.

⁵⁴ CMS, [Medicaid Payment Suspension Toolkit](#), October 2014.

⁵⁵ 42 CFR 431.51(c)(2). Qualification standards must be related to the provider's fitness to perform covered medical services or to appropriately bill for those services.

⁵⁶ 42 CFR 455.106(c).

⁵⁷ Ohio Administrative Code, Rule 5160-1-17.6 [Termination and Denial of Provider Agreement](#), paragraph G, effective April 9, 2015.

Beneficiary Lock-in. Bad actors can also include some beneficiaries and/or their families who purposefully exaggerate or feign disability to obtain unneeded services, collude with providers to sign blank or false timesheets for a kickback payment, or “shop” PCS agencies to find one that will obtain authorization for more services or pay a friend or family member more to provide care in programs where family care can be paid for by Medicaid. State Medicaid Agencies lack strong tools for sanctioning beneficiaries, but some effective methods can be used. The SMA can lock-in colluding beneficiaries to a specific trusted agency, in accordance with regulatory requirements at 42 CFR 431.54(e). Likewise, if beneficiaries or their families are allowing attendants who are friends, family members, or live-in caregivers to provide less than the full complement of paid services, the SMA can lock-out the offending caregiver and provide services from a trusted PCS agency.

Risk: Fraudulent providers and colluding beneficiaries

Vulnerabilities

- Payments being made while fraud investigations are ongoing, except in cases where the state finds good cause not to suspend payments according to 42 CFR 455.23(e).
- Payments being made to suspect, fraudulent, or inappropriate providers (e.g., providers with fraudulent disclosures, excluded affiliations, or terminated by Medicare or other states).
- Payments for unneeded services due to some beneficiaries purposefully exaggerating or feigning disability or colluding with providers.
- Family and/or live-in caregivers failing to provide the full complement of paid services.
- Providers terminated for noncompliance re-applying for enrollment.

Mitigations

- Use prepayment review as a sanction and monitoring tool for providers with problematic billing practices.
- Use authority to suspend payments pending investigations of credible allegations of fraud and coordinate with the MFCU to resolve cases timely to take appropriate follow-up action.
- Work with the MFCU to investigate fraud violations, terminate fraudulent providers, and build cases for prosecution. Report any terminations to CMS after the provider has exhausted all appeal rights or the timeline for appeal has expired.⁵⁸
- Lock-in colluding beneficiaries to a specific trusted agency, in accordance with 42 CFR 431.54(e).
- Lock-out caregivers who fail to provide full paid services, in accordance with 42 CFR 431.54(f).

⁵⁸ See “Medicaid Termination Reporting,” in: CMS, [Medicaid Provider Enrollment Compendium](#) (MPEC), June 2017.

- For previously terminated providers re-applying for enrollment, check disclosure information, check other sources for required but undisclosed information, conduct site visits to check disclosure information and evaluate compliance, and deny enrollment if noncompliant using available authorities [42 CFR 455.106(c)]. Use authority to obtain disclosure of information related to business transactions to reveal potential straw owners or other kickback relationships [42 CFR 455.105]. Strengthen state standards relating to the qualifications of providers using authority under 42 CFR 431.51(c)(2), and deny enrollment when standards are not met (see also [text box](#) on Ohio's best interest authority).

Streamline referral and investigation of suspected fraud

Consensus from MII participants was that states could make considerably more headway in identifying and recovering improper payments, investigating and prosecuting fraud, and terminating and convicting proven offenders by instituting more effective interagency collaboration.

One vulnerability cited was that providers had been able to exploit the lack of coordination between the SMA and MFCU. For example, a provider under investigation by the MFCU claimed not to have understood certain responsibilities regarding maintaining documentation of services, leading prosecutors to doubt the strength of their case against the provider. Fortunately, after the provider's excuse came to the attention of the Medicaid program integrity staff, prosecutors were informed that the SMA had provided explicit training and documentation to the provider on the exact documentation requirements. For this reason, MII participants recommended collecting signatures from providers attending training, attesting to having attended and understood their responsibility for the content. To alleviate the vulnerability, participants recommended interagency training to familiarize staff in all relevant agencies with policies and operations of other agencies.

MII participants also recognized the need for better coordination between the SMA and MFCU in handling referrals of potential fraud. The process of making quality referrals, making timely decisions about whether or not to accept referrals, tracking case progress, keeping up-to-date about the status of referrals, and communicating decisions regarding credible allegations of fraud and payment suspensions were all issues of concern to MII participants. Mitigations such as strengthening collaboration through regular meetings, sharing data and resources, and developing interagency case tracking databases are listed below. CMS has published guidance documents to assist states in meeting challenges of SMA-MFCU interactions on fraud referrals and on consultations specifically regarding payment suspensions.^{59,60}

⁵⁹ CMS, [Best Practices for Medicaid Program Integrity Units' Interactions with Medicaid Fraud Control Units](#), September 2008.

⁶⁰ CMS, [Medicaid Payment Suspension Toolkit](#), October 2014.

Risk: *Weak interagency collaboration hampering recovery efforts and fraud prosecutions*

Vulnerabilities

- Poor collaboration and inconsistent policy interpretation within and between agencies (e.g., SMA, MFCU, licensing agencies, Labor Department).
- Difficulty in sharing information and resources among state agencies.
- Lack of knowledge about how other state offices or agencies operate allows providers to exploit poor interagency cooperation by giving false exculpatory information.
- Fraud referrals with missing information or inadequate documentation.
- Late or lacking feedback to offices that originate referrals. Delays in decisions whether or not to pursue a case referral prevents the referring agency from pursuing overpayment recovery.

Mitigations

- Strengthen collaboration between the SMA and the MFCU to improve referrals and better coordinate investigations based on credible allegations of fraud to promptly resolve provider payment suspensions.
- Collaborative meetings among agencies (SMA and MFCU) lead to sharing information and sharing resources: data and data analytic capability in one agency can provide needed resources and information for other agencies to achieve common goals.
- Regular meetings between the MFCU and SMA may help assess when the deterrent value and sentinel effect of prosecution of intransigent low-level offenders may be worthwhile even when overpayment recovery may be modest.
- Streamline and simplify interagency data use agreements to more effectively share data among state agencies (e.g., incarceration and court records, employment records, and business and health practice licenses).
- Organize interagency training on respective policies, functions, and provider interactions.
- Develop or improve a tracking system and/or shared database for the SMA and MFCU to track the progress of referrals and cases cooperatively.
- State staff who enroll or monitor providers or review claims (pre- or post-payment) should have training to understand the importance of accurate data and data analysis in support of screening, investigations, and referrals.
- Organize state policy workgroups to include all stakeholders to review regulatory and policy changes, so that writers of policy have input from enforcers of policy—e.g., from program integrity staff and the MFCU.

Personal care services in Medicaid managed care

Implement parallel safeguards in managed care contracts

Personal care services provided through Medicaid managed care contracts are subject to the same vulnerabilities as listed above for Medicaid fee-for-service programs. Accordingly, SMAs' contracts with managed care entities should include language requiring the same safeguards outlined above in all of the following areas:

- Screened and qualified providers, with attendant information listed in a caregiver registry
- Face-to-face functional needs assessments and reassessments by qualified independent agents
- Complete and accurate documentation of services
- Complete service specifications on encounter claims (units of service for each date of service; attendant identifier as the rendering provider)
- Effective prepayment review to block payment for services not authorized or not in accordance with policy (e.g., PCS during inpatient stays)
- Periodic provider and beneficiary education on fraud, waste, and abuse issues
- Post-payment data analysis to identify potential improper payments
- Audits and investigations to identify and recover overpayments
- Referrals of suspected fraud to the state and MFCU
- Reporting of adverse administrative actions against provider participation to the state
- Regular meetings and effective coordination with the SMA's program integrity unit

Closing Remarks

The foregoing consensus recommendations developed by the diverse group of state and federal Medicaid and law enforcement experts at the MII course provide a roadmap to help states strengthen their safeguards to protect vulnerable beneficiaries and reduce improper payments in Personal Care Services. By implementing these mitigation strategies, state Medicaid programs can work to more effectively monitor and control who can provide services for beneficiaries in their homes and bill for Medicaid payment; ensure that beneficiaries receive valid assessments to authorize needed services; validate that services were provided in accordance with approved plans of care; and detect, terminate, and prosecute fraudulent providers.

These mitigation strategies were identified by experts primarily drawn from state agencies as practical and achievable. Most recommended mitigations have been implemented with success in a number of states, as noted in the narrative. While challenges of implementing improvements exist, CMS offers technical assistance to states in accessing needed expertise within CMS, as well as obtaining information about effective practices in other states. Inquiries regarding obtaining technical assistance can be directed to CMS Medicaid program integrity staff at Medicaid_Integrity_Program@cms.hhs.gov.