Deloitte.

Strengthening Long-Term Services and Supports (LTSS) Program Integrity: Protecting Access, Quality, and Public Funds

WHY NOW

LTSS program integrity is receiving increased attention as a quality, access, and public funds concern

WHAT IS LTSS PROGRAM INTEGRITY?

For LTSS agencies, program integrity means that services are authorized, delivered, documented, and billed accurately and effectively, reducing potential fraud, waste, and abuse (FWA).

THE CORE INTEGRITY RISKS

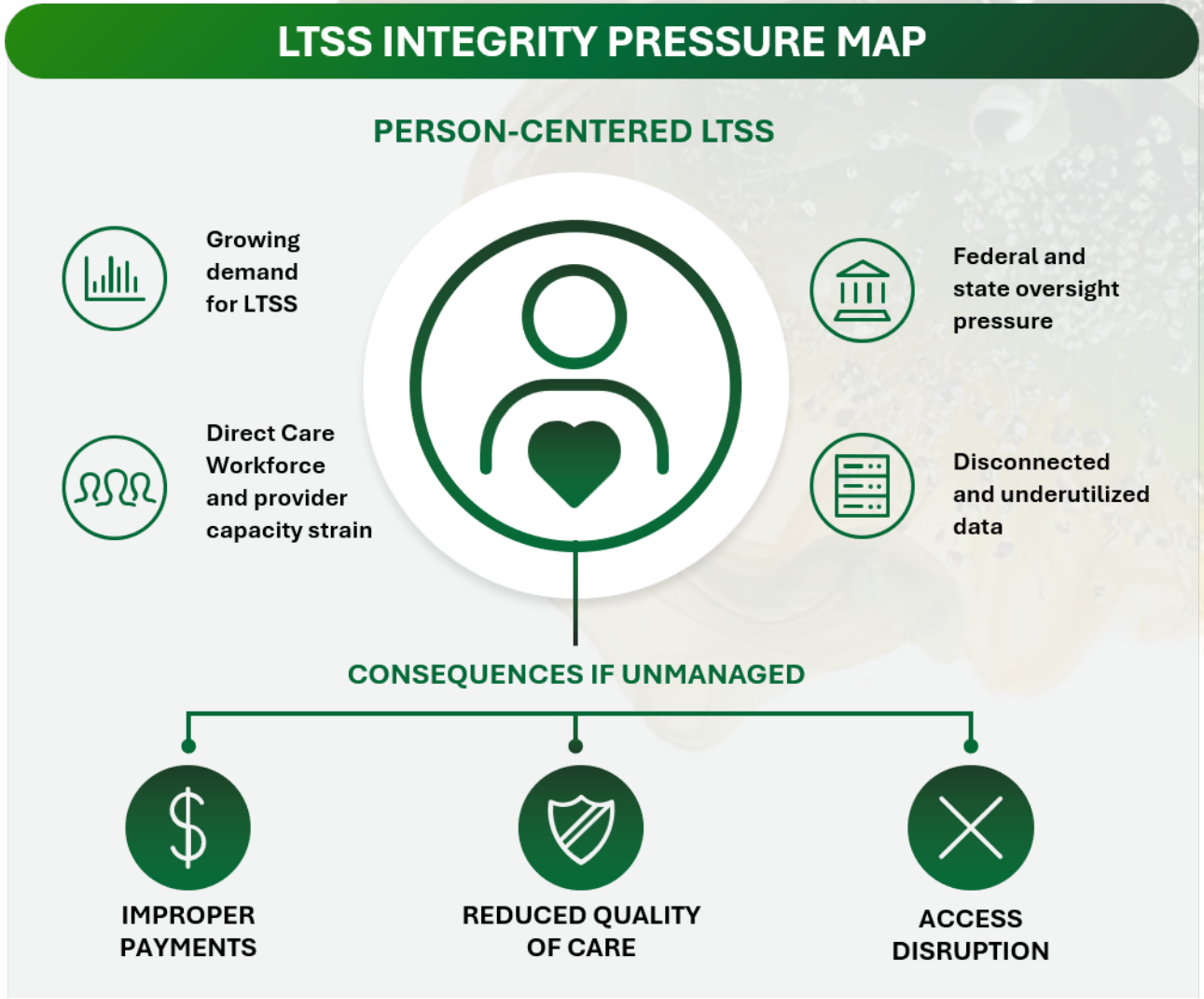
Fraud - Intentional deception to obtain an unauthorized LTSS benefit or payment.

Waste - Unnecessary LTSS spending caused by inefficient or avoidable practices.

Abuse - Unauthorized LTSS practices that create Medicaid cost or pay for unnecessary or substandard services.

LTSS integrity is broader than claims review. Integrity helps states confirm that people receive authorized supports they are eligible for without disrupting access while safeguarding public trust

LTSS is growing, shifting toward home and community-based settings, and operating under increased federal and state oversight, workforce strain, and data fragmentation.



WHERE RISK CONCENTRATES

LTSS program integrity breaks in the gaps between the plan, the service, the provider, and the oversight model

HIGH-VALUE INTEGRITY OPPORTUNITIES

are targeted checks where LTSS programs often lose visibility: whether the support was planned, delivered, documented, billed by the right provider, and visible to the state.

FOUR PLACES LTSS INTEGRITY BREAKS

Plan-to-claim mismatch - Claims may pass system checks but exceed or drift from authorized based on the person-centered plan.

What to check: Claims vs. person-centered plan, authorized units, assessed need, service mix, and repeated max-unit billing.

Opaque service delivery - In-home, community, transportation, respite, and self-directed services can be hard to observe.

What to check: Electronic-Visit Verification (EVV) exceptions, care provider overlap, participant feedback, incident patterns, remote supports data, and claims during inpatient/facility stays.

Provider identity and ownership gap - Risk can hide across shared owners, related entities, fiscal intermediaries (FIs), staff, addresses, phone numbers, or excluded individuals.

What to check: Ownership, enrollment, credentialing, exclusions, shared identifiers, rapid billing growth, and related-party relationships.

Delegated oversight - In LTSS in managed care (MLTSS), FI-supported, and provider-managed models, the state may not see risk until after payment or harm occurs.

What to check: Managed Care Organization (MCO) encounter quality, Special Investigations Unit (SIU) referrals, payment suspensions, provider terminations, FI controls, complaints, and recoveries.

LTSS RISK-CONTROL MATRIX

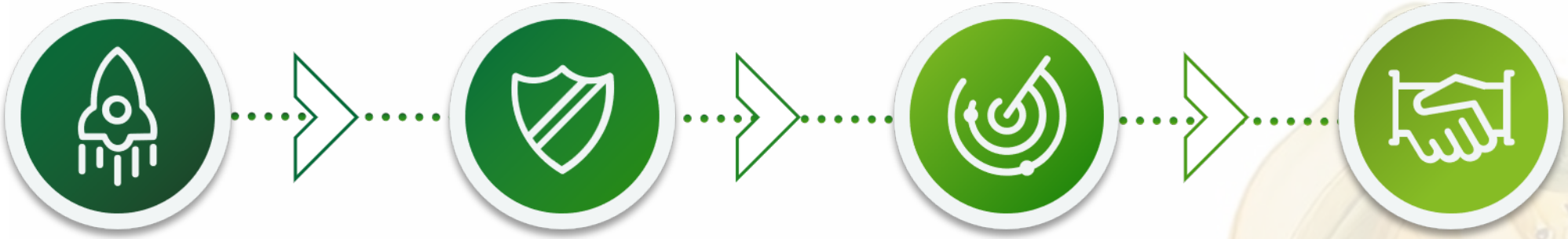
LTSS RISK POINT	WHAT CAN GO WRONG	BETTER CONTROL QUESTION	PRACTICAL CONTROLS
PERSON-CENTERED PLAN	Claims fit a system cap but not the person's authorized plan	"Does the claim match personal goals and authorized supports?"	Service-plan-to-claim checks, participant input, max-unit outliers, plan quality review
HOME / COMMUNITY DELIVERY	Services are billed but not delivered, or delivered by the wrong staff	"How can we verify that service was delivered, and delivered as intended?"	EVV exceptions, worker overlap checks, participant/family feedback, education
INSTITUTIONAL LTSS	Payment and quality risks hide in staffing, assessments, ownership, and cost reports	"Do payment, staffing, quality, and ownership signals tell a consistent story?"	Staffing / survey / assessment / ownership / cost-report analytics
MLTSS / DELEGATED OVERSIGHT	Risk is managed by plans, FIs, or providers before the state sees it	"Do delegated partners detect, report, and resolve issues proactively?"	Encounter review, SIU benchmarks, FI audits, contract levers
TRANSITIONS AND ELIGIBILITY	Payments continue after hospitalization, facility admission, death, or eligibility change	"Could this service have occurred on that date?"	Inpatient, facility, death, eligibility, and transition overlap checks

Participants and their families can help prevent and identify issues when they have service information, ways to share feedback, and a role in resolution. Empower them with the tools and information to be program integrity partners.

WHAT STATES CAN DO NOW

States can start with practical, targeted actions using data they already have and build toward an LTSS-wide integrity model that identifies problems earlier, responds proportionately, and protects access

LTSS PROGRAM INTEGRITY OPERATING MODEL



1. ASSESS

Segment risks by provider, service, population, geography, and access impact using available data

2. PREVENT

Strengthen provider screening, education, ownership transparency, and prepayment controls

3. DETECT

Connect claims, EVV, authorization, encounter, staffing, and quality data to surface anomalies and prioritize leads

4. RESPOND

Match the response to the root cause, education, technical assistance, corrective action, recovery, or referral, and monitor access

Governance, data-sharing agreements, MCO/FI accountability, human-in-the-loop analytics, and access safeguards

DELOITTE ENABLERS

FWA Maturity Assessment Model: Assess maturity across policy, controls, analytics, delegated oversight, and operations	**Technology-enabled program integrity**: Pallium™ and HealthInteractive™ connect data, analytics, oversight, and case management	**Policy and program strategy**: Set risk priorities, control objectives, and an access-sensitive roadmap
Data integration and analytics: Link claims, EVV, authorization, encounter, provider, and outcome data	**Operating model and governance**: Clarify roles, workflows, escalation paths, and oversight across the LTSS ecosystem	**Change management and provider education**: Translate findings into targeted education, technical assistance, and sustained adoption

Deloitte.