

ALPRP Technology Framework

Five Stages. One Correctional Journey.

Public-facing proposed policy | October 5, 2026

ALPRP proposes a connected technology framework that supports resident safety, mental-health care, education, professional correctional staff, victim services, family preparation, and successful reentry. Technology will help Alabama identify needs, deliver services, document responsibility, and evaluate results across Revive, Rehabilitate, Rebuild, Restore, and Release.

This framework is a proposal, not an adopted Alabama Department of Corrections policy. ALPRP applications are prototypes or proposed tools. Commercial products named here are examples for evaluation, not endorsements or confirmed purchases. Every operational deployment requires appropriate authorization, supported equipment and interfaces, security review, trained personnel, and acceptance testing.

Our purpose

The purpose is safer institutions and safer communities. Residents need protection, treatment, education, and a clear path toward responsibility. Officers need reliable equipment, manageable workflows, training, and support. Victims need services centered on their safety and healing. Families and community providers need practical preparation. The public needs trustworthy evidence of performance.

ALPRP will measure both resident progress and institutional performance. A missed appointment must show whether the resident declined it or whether an escort, provider, device, or facility restriction prevented access. A completed scan must not be mistaken for completed care. An unanswered alert must not disappear into a dashboard.

Technology will support people. Qualified people will make clinical, custody, disciplinary, educational, parole, and progression decisions.

ALPRP will judge technology by whether residents receive safer, timely, respectful care and verified opportunities to progress. Monitoring will be limited to justified purposes, reviewed regularly, and reduced or discontinued when unnecessary or harmful. Equipment will never substitute for required staffing, direct observation, treatment, or fair human decisions. These protections apply to pilot operations, procurement contracts, technical settings, staff procedures, and independent review.

The tools and their roles

Tool or service	Proposed role
Saharah Compass	The resident-facing guide to approved schedules, expectations, goals, resources, supportive exercises, requests for assistance, and documented progress.
Guard1 or another approved tracking and verification system	Monitored-zone information, assigned-device records, physical identification scans, selected movement alerts, and documented operational checks.
Medical monitoring wearables	Selected physiological readings and notifications for residents whose assessed clinical needs justify monitoring with a validated, appropriate device.
Staff emergency devices	A way for designated personnel to request help and identify the monitored zone associated with an emergency activation.
Secure tablets and computer labs	Approved access to learning, support tools, information, and communication. Devices must support accessibility and the intended applications.
Learning management system, or LMS	Enrollment, coursework, assessments, instructor-confirmed participation, competencies, and credentials.
Virtual reality and vocational simulators	Supervised practice in occupational skills, decision-making, and appropriately validated therapeutic exercises.
Telehealth, teletherapy, and clinical records	Professional assessment, treatment access, appointment coordination, and continuity of care.
Shield & Standards	Officer wellbeing, confidential support pathways, training, professional development, workplace-risk review, and fair accountability.
Haven Alabama	Victim-directed crisis resources, counseling and assistance navigation, safety planning, case information, and voluntary restorative options.
Family Connect	Approved institutional information, document organization, communication guidance, and practical reentry preparation.
Covenant Connect	Coordination of vetted providers and confirmed housing, employment, transportation, healthcare, treatment, and other community commitments.
Parole Packet Assistant	Organization of verified achievements, supporting documents, and release plans for review by people responsible for the process.
ALPRP progression records	Individual plans, approved progress summaries, panel reviews, decisions, reasons, and correction or appeal records.
Community Repair coordination	Records of approved projects, supervision, skills, verified work, and community contributions. Community repair is a service pathway, not a claim that a dedicated application is already operational.
Transparency Dashboard	Public reporting of reviewed, appropriately aggregated service, safety, workforce, and outcome information.
Reform Coach and Ask ALPRP	Public explanation, research support, and advocacy tools that distinguish official evidence, reported concerns, analysis, proposals, and illustrative prototypes.

Saharah Compass provides supervised support and educational guidance. Its AI features do not make it a licensed clinician or replace professional assessment and treatment.

How the plan follows the stages

Stage	Technology contribution
Revive	Identity verification, assessment coordination, safe routines, clinical monitoring when indicated, treatment access, orientation, and protected requests for help.
Rehabilitate	Frequent education and treatment, verified service access, supervised simulations, supportive exercises, and documented achievement.
Rebuild	Advanced learning, supervised paid work inside the facility, mentoring, and verified competencies. This stage does not authorize off-site work.
Restore	Approved transitional activity, family preparation, community repair, employer and provider coordination, and documented departure and return.
Release	Confirmed housing, employment preparation, healthcare appointments, treatment continuity, credentials, supervision requirements, and community support.

Clinical monitoring may begin, continue, or end in any stage according to reassessed need. Progression will not automatically require a device change. After release, any monitoring requires its own lawful authority, purpose, limits, and review. Reentry support will not become indefinite surveillance by default.

Identification, movement, and daily schedules

Officers will verify the resident before assigning an identifier or wearable. Issue, replacement, transfer, and return will be documented. Residents will not be matched across systems by name alone.

Physical counts will remain. Officers will visually verify residents and use approved scanning procedures to support reconciliation. Location information can help direct a search when records do not match, but a detected bracelet does not independently prove that its assigned resident is present or safe.

Approved schedules will identify activities, destinations, times, and relevant escort or separation requirements. Staff will record departure and arrival where required. Unexpected movement will trigger verification and an appropriate response, not automatic discipline.

Indoor tracking requires a tested receiver infrastructure. It is not off-site GPS. Resident-operated emergency buttons, two-way wearable communication, and off-site monitoring are separately specified capabilities; they will not be implied by purchasing a tracking tag.

Separation and movement requirements will follow individualized, approved decisions. A stage label alone does not establish that residents can safely interact.

Education, treatment, and progression

The systems will preserve the difference between being scheduled, being physically present, participating, and completing a task. Educators assess learning. Clinicians assess treatment. Authorized panels review stage progression.

If instruction or treatment is missed, the record will distinguish refusal from illness, lockdown, scheduling conflicts, unavailable escorts, provider cancellations, and technical problems. Staff will arrange appropriate follow-up and protect earned achievements from inaccurate records.

AI may explain instructions, support approved exercises, help draft documents, and summarize authorized information. It will not determine diagnosis, dangerousness, credibility, punishment, housing, parole, or stage advancement. It will not invent certificates, treatment participation, employment offers, or other evidence.

Private reflections and clinical conversations will not automatically become progression or parole evidence. Residents can use approved, reviewed achievement summaries without surrendering all private support content. No automatic AI emotional or behavioral score will be used to rank release readiness.

Mental-health care and medical monitoring

Revive will prioritize assessment, stabilization, safe placement, treatment access, and meaningful human contact. Mental-health needs will continue to receive attention throughout every stage, including after transfers and during release preparation.

Qualified clinical personnel will determine whether a resident needs physiological monitoring, what equipment is appropriate, and what treatment and observation are required. Monitoring will follow assessed need rather than automatically apply to everyone with a diagnosis or everyone in a particular stage.

Potential products include custody-oriented systems such as OverWatch and medical monitoring products such as Biobeat. The exact model, supported measurements, regulatory status and intended use, attachment safety, accuracy, and correctional suitability must be verified. One product's capability or clearance will not be attributed to another product or model. Manufacturer pages are not independent clinical validation or proof of suitability for Alabama facilities.

A medical wearable may provide additional warning of concerning physiological changes. It will not independently diagnose panic, psychosis, depression, aggression, overdose, or suicidal intent. Pacing, inactivity, and changes in vital signs have multiple possible explanations. They will prompt appropriate assessment rather than labels or punishment.

Required direct observation, suicide-prevention procedures, clinical assessment, medication continuity, and treatment will continue. Normal readings will not override a resident's request for help or observed distress. Monitoring will not justify fewer required staff observations, isolation, or delayed transfer to appropriate care.

Clinical teams will consider medications, medical conditions, individual history, and the resident's baseline. An abnormal intake measurement will not become an acceptable baseline merely because it was recorded first. Devices must be evaluated for relevant accuracy limitations, including skin pigmentation, movement, contact, and missing signals.

Separate identification, movement, and clinical monitoring

A resident may need a scannable identity device or authorized movement verification without needing continuous physiological monitoring. Each function requires its own purpose, authority, access rules, and acceptance test. A combined device does not authorize every available sensor. Unnecessary functions must be disabled, and tests must confirm that disabling ends collection, storage, and transmission as intended.

Clinical monitoring requires a documented assessment by qualified clinical personnel. The record will explain the concern, expected benefit, less intrusive alternatives, device suitability, duration, next review, and removal criteria. A diagnosis or stage assignment alone does not justify monitoring. Clinical need is separate from discipline and program readiness; residents do not have to demonstrate perfect vital signs or stop requesting help to progress.

Meaningful explanation, choice, and alternatives

Before optional clinical monitoring begins, residents will receive an accessible explanation of what is collected, why, who can see it, how long it is retained, known limitations, physical risks, alternatives, and how to withdraw or complain. Provide language assistance, disability accommodations, and an opportunity to ask questions. A signed form alone does not demonstrate understanding or voluntary choice.

Declining or withdrawing from optional monitoring must not reduce access to appropriate care, education, privileges, or progression opportunities. Clinicians will arrange a clinically appropriate alternative care and observation plan. Optional monitoring will not be described as voluntary if refusal results in punishment or loss of necessary services.

Any compulsory use requires a documented lawful basis, clinical justification where applicable, the least intrusive suitable approach, a defined review period, and a way to challenge the decision. Urgent care follows approved emergency and legal procedures. ALPRP does not promise that all legally authorized custody measures are optional.

A care pathway that works without a sensor

Requests through Saharah Compass, direct resident reports, staff observations, and clinically relevant device alerts will all lead to an accountable response. Residents must have a readily available way to request help when a tablet, network, or wearable is unavailable. Normal readings must never override reported distress.

The responsible team will receive the concern, assess urgency, arrange professional assessment, document a care plan, deliver the required services, and verify follow-up. Scheduling tools will support counseling, medication continuity, teletherapy, education accommodations, and safe handoffs after moves and release. A clinical record will hold the clinical assessment; shared operational records will contain only the instructions necessary to deliver services.

The pilot will measure requests for help, time to assessment and treatment, missed services and their causes, required observations, continuity of care, and resident-reported ability to obtain help. More alerts or more data are not themselves evidence of better treatment.

Safe attachments, hygiene, and removal

Procurement must evaluate the complete device and attachment for prolonged skin contact, fit, cleaning, pressure, circulation, allergy and irritation risks, foreseeable misuse, ligature hazards, and emergency removal. Tamper resistance and self-harm safety are separate requirements. Labels such as medical-grade silicone, ballistic resin, or hypoallergenic do not establish that the finished device is safe for every resident.

Staff will arrange daily skin checks and hygiene opportunities consistent with device instructions and clinical needs. Pain, swelling, numbness, skin damage, or an unsafe attachment requires prompt clinical assessment and removal or adjustment when indicated. Staff will not delay necessary removal to preserve tracking data. An alternative observation or protection plan must cover removal, charging, replacement, and repair. Repeated injuries trigger review of the device model and pilot suitability.

Monitoring reduction and supported self-management

Medical monitoring, custody identification, movement tracking, and community supervision serve different purposes. Ending one does not automatically end the others. Each requires a documented purpose, appropriate authorization, access safeguards, and review. Residents may advance through ALPRP while continuing medically necessary monitoring, or stop medical monitoring before advancing to another stage.

Revive and Rehabilitate: assessment, treatment, and regular review

Revive prioritizes assessment and stabilization. Rehabilitate provides structured education, counseling, treatment, and practice in responsibility. Selected residents may receive wearable monitoring as a supplement to professional care in either stage.

ALPRP proposes weekly documented reviews while continuous medical monitoring remains in use, with earlier review after significant changes. Responsible clinical leadership must approve the final schedule. This is an administrative proposal, not a validated universal clinical interval. Review must never delay a needed change in care.

Reduction depends on current assessment, treatment response, recent clinically verified events, and available support. An absence of alerts does not establish stability. False alerts, physical illness, side effects, unavailable treatment, disability needs, or seeking help will not automatically prevent progression or monitoring reduction. Medication decisions remain clinical decisions; disciplinary findings receive a separate human review.

Rebuild: supported independence inside the facility

Stage 3 remains inside the correctional facility. Residents participate in advanced education, supervised paid work, approved mentoring, and transition preparation. Rebuild does not authorize off-site work release.

Medical monitoring may continue, become intermittent or limited to a documented clinical circumstance, or end when its expected benefit no longer justifies its burden. Overnight monitoring is not automatic. A

parole hearing or housing change does not by itself justify renewed biometric collection. The clinical team determines whether additional support or monitoring is appropriate.

A less restrictive attachment may be considered only when the approved device supports it and testing establishes suitability. Procurement and clinical teams must verify whether changes in sampling, transmission, attachment, or operating mode are actually supported. Every approved change is documented and tested before use.

When medical collection is stopped, the system must clearly identify it as inactive. Stopping transmission alone does not establish that the device stopped recording or storing data. The technology team verifies the intended behavior and explains any continued storage or connectivity. A connectivity signal confirms a device connection, not the resident's presence, wellbeing, or safety.

Physical counts, authorized identification, and appropriate custody controls continue independently. Residents receive explanations of remaining monitoring and access to the applicable record-correction process.

Restore: transitional activity and continuity of care

Stage 4 provides approved transitional opportunities, including off-site work or furloughs where authorized. Restore remains structured; it does not automatically confer unrestricted community autonomy.

Before transition, the team verifies the current clinical plan, any remaining monitoring need, medication access, provider handoffs, confirmed appointments and transportation, movement permissions, supervision requirements, and emergency contacts. Saharah Compass supports schedules, learning, reminders, service navigation, and requests for assistance, with accessible alternatives.

Medical wearables are removed when clinically appropriate. Continued monitoring requires documented justification and review. Removing the device ends on-body sensing for that resident; staff must separately deactivate or reassign it and verify remaining recording, storage, and transmission behavior; existing records remain subject to approved retention and access rules. Records are not automatically deleted, and unrelated custody or legally authorized supervision requirements are not automatically ended.

Release: community self-management with practical support

Stage 5 shifts care toward community providers and resident self-management, supported by confirmed housing, healthcare, treatment, transportation, and supervision handoffs. Scheduling assistance and accessible services remain available according to need. Residents will not be expected to manage unavailable services independently.

Any community location monitoring requires separate lawful authorization. ALPRP participation alone will not justify indefinite tracking. Check-ins use the least intrusive effective method, such as secure account access, telephone contact, an approved kiosk, or in-person verification. Saharah Compass will not replace licensed clinicians or legally authorized supervision personnel.

Biometric check-ins require a separate privacy, security, accessibility, and authorization review. ALPRP will provide a non-biometric alternative. Facial or voice authentication does not independently establish location or curfew compliance. Failed check-ins prompt verification of connectivity, access, disability

needs, and circumstances before any adverse conclusion. Identity records and any separately authorized location evidence must be evaluated for accuracy by people.

Crisis response and temporary increases in support

A new crisis triggers assessment, care, and protection. It does not automatically trigger punishment, loss of achievements, a device replacement deadline, or a reset of a 30-day clock.

1. Staff respond immediately under approved emergency procedures.
2. Qualified personnel assess risk and required treatment or observation.
3. Clinicians determine whether additional monitoring would be useful and safe.
4. Custody personnel coordinate necessary placement changes through authorized procedures, using the least restrictive appropriate arrangements.
5. The team documents the reason, resident explanation, responsible decision-makers, review date, and conditions for reducing restrictions.

A wearable must never delay emergency treatment, required observation, or hospital transfer. Relapse, distress, or requests for help will not automatically erase educational achievements or determine misconduct. Any genuine disciplinary allegation is considered separately, with evidence, accommodations, and applicable review safeguards. Clinical personnel direct clinical monitoring; a multidisciplinary team coordinates services without overriding clinical judgment on medical need.

Accountability for monitoring reduction

Pilot 100 will add the following measures to its scorecard. Targets are proposed service obligations, not guarantees of clinical outcomes.

Indicator	Definition and verification	Proposed goal
Justified monitoring duration	Medical monitoring days and resident-days, with documented indication, responsible clinician, and next review date; audit active orders against actual collection.	100% of active clinical monitoring supported by a current documented plan.
Timely clinical review	Reviews completed by the approved due date divided by reviews due; report overdue cases and reasons.	100% of required reviews; earlier reassessment when needs change.
Timely change implementation	Time from an approved reduction or discontinuation order to verified device and system change; report median, 90th percentile, maximum, and failures.	Meet a defined implementation deadline for each order; investigate delay and continued unauthorized collection.

Indicator	Definition and verification	Proposed goal
Safety after a monitoring change	Confirmed adverse events, missed alerts where monitoring remained ordered, unplanned increases in support, and treatment interruptions within pre-specified follow-up windows, such as 7 and 30 days.	Independently review serious events; do not attribute causation without evidence or reward avoiding appropriate step-down.
Treatment continuity and access	Confirmed handoffs and services received; record failures in appointments, medications, transport, and accessible alternatives.	Verify all required handoffs and promptly remedy barriers.
Privacy, understanding, and fairness	Complaints, corrected records, resident understanding, and lawful protected analysis of monitoring duration and service access across groups.	Explain every monitoring plan, provide a complaint pathway, and investigate unjustified differences or collection.

Publish aggregate findings while protecting small groups and sensitive records. Success means appropriate monitoring, safe reductions, sustained care, and supported responsibility. The percentage of devices removed is not a stand-alone success measure.

Alert levels, response deadlines, and escalation

Every alert or reported concern will have a responsible role, deadline, backup, and escalation route. Clinical and custody concerns require appropriate verification; routine administrative alerts may be resolved without a physical resident check. Serious incidents and near misses require evidence preservation and accountable review.

ALPRP proposes four alert levels for Pilot 100. Level 1 has the highest urgency. These are proposed operating targets, not established ADOC standards or clinically validated deadlines. Clinical, custody, and technology leadership must approve the protocols and demonstrate adequate staffing, coverage, and backup arrangements before launch.

Staff act immediately when danger is apparent. A deadline is not permission to wait. A stricter clinical order or approved emergency procedure takes precedence. Responding means assessment or protective action, not opening a dashboard.

Level and meaning	Acknowledge and assign	Required response
Level 1 - Critical: immediate or suspected threat to life or serious harm	Immediate dispatch; acknowledgement within 30 seconds.	Intervention begins immediately where staff are present. Proposed first qualified responder arrival under 3 minutes; emergency clinical support activated immediately. Record arrival, resident access, and care separately.
Level 2 - Urgent: significant concern needing prompt assessment without an established immediate life threat	Within 2 minutes.	In-person safety assessment within 10 minutes. Clinical assessment initiated within 15 minutes when clinically relevant, sooner if indicated.
Level 3 - Priority: non-emergency concern that could disrupt care, safety, or services	Within 15 minutes.	Initial assessment or protective action within 60 minutes; documented plan within 4 hours.
Level 4 - Routine: administrative, maintenance, or scheduled support without current safety consequences	Within 4 hours.	Review and action plan within 24 hours; completion by a documented due date.

Clocks start at alert generation or first staff receipt of a reported concern. Retain detection and delivery times, including transmission delays. Act immediately on observed danger. Drills verify resident access and intervention as well as arrival.

Alert types and responsible responses

Alert or concern	Default level	Required action and responsible role
Unresponsiveness, suspected overdose, serious breathing difficulty, collapse, or apparent medical emergency	1	Officers activate emergency procedures and provide assistance within their training; clinical personnel respond and activate EMS when indicated. Do not wait for wearable confirmation.
Active self-harm, suicide attempt, or credible imminent self-harm concern	1	Immediate protection, emergency clinical assessment, and required observation. A wearable supplements care.
Critical physiological alert under an approved clinical device protocol	1	Immediate resident assessment and clinical response. Thresholds depend on the validated device and individual plan.
Officer panic button, active assault, serious threat, or weapon emergency	1	Control room dispatches the designated response team; supervisor coordinates protection and medical assistance.
Missing resident with credible escape, abduction, or immediate danger indicators	1	Activate approved custody emergency procedures and physical verification.
Required continuous observation interrupted, or critical monitoring lost without adequate protection	1	Restore required human protection immediately; assess the resident and activate backup arrangements.
New distress, worsening withdrawal symptoms, or concerning physiological change without apparent immediate danger	2	Prompt officer safety check and clinical triage. Initiate appropriate assessment and upgrade immediately if danger emerges.
Pacing, inactivity, or another movement anomaly with context indicating concern	2	Verify condition and obtain clinical assessment as appropriate. Movement alone does not establish psychiatric illness or misconduct. Isolated low-risk technical anomalies receive a context-appropriate level.
Unexplained signal loss from a clinically monitored resident	2	Verify wellbeing and restore the approved monitoring or observation arrangement. Level 1 if immediate risk or required protection is compromised.
Unresolved count discrepancy, unauthorized movement, or separation-plan alert	2	Custody physically verifies identity, location, permission, and safety. Upgrade for credible immediate danger.

Alert or concern	Default level	Required action and responsible role
Overdue required welfare check	2	Perform the check immediately on discovery; supervisor investigates. Level 1 if continuous observation or immediate safety is compromised.
Missed medication or interrupted treatment	2 or 3, clinically assigned	Clinical personnel determine urgency and corrective action. Time-critical medication or serious deterioration requires higher priority.
Critical system outage with effective manual protection operating	2	Operations maintains manual procedures; technology staff assess and contain the failure. Level 1 if protection fails.
Suspected active cyberattack, unauthorized disclosure, or corrupted safety records	2	Security lead begins containment and preserves evidence; operations verifies safe continuity. Level 1 if immediate physical safety is affected. Separate notification obligations remain applicable.
Low battery with adequate monitoring available	3	Device team inspects, charges, or replaces before the validated remaining operating window expires. Upgrade if coverage is threatened.
Device discomfort, skin irritation, or attachment concern	3	Clinical assessment and safe adjustment or removal. Serious injury, circulation concern, or immediate attachment danger requires Level 1 or 2.
Identity mismatch, stale roster, or conflicting progression record without immediate danger	3	Verify authoritative records, suspend adverse decisions based on disputed information, and correct affected systems.
Missed education, counseling, escort, or appointment due to a service barrier	3	Service owner records the cause and arranges recovery. Upgrade according to clinical urgency.
Failed community check-in without evidence of danger	3	Authorized personnel verify connectivity, access, circumstances, and supervision requirements before drawing conclusions.
Alleged past misconduct without a current safety threat	3	Supervisor preserves evidence and routes it through human review. An alert is not a finding of guilt.
Routine scheduling, course reminder, or nonessential repair	4	Relevant service owner reviews and assigns a completion date.

Alert or concern	Default level	Required action and responsible role
Monitoring review reminder	4 before due date; 3 when overdue	Clinical team completes the required review. An unsafe current plan requires higher-priority assessment.
Approved monitoring reduction or removal order	3 unless clinician directs faster action	Clinical and device teams implement by the specified deadline and verify device and system collection behavior.

Complaints about violence, retaliation, abuse, or denied care are classified by underlying risk, not automatically treated as routine. Uncertain clinical urgency is promptly referred to a qualified clinician; staff do not downgrade apparent danger while awaiting confirmation.

Escalation and authority

Level 1 dispatches primary and backup responders simultaneously. If acknowledgement is absent at 30 seconds, notify the shift commander and clinical emergency lead through an independent channel. Immediate protection continues while additional help is dispatched.

Level 2 unacknowledged alerts escalate at 2 minutes; missed response deadlines escalate to the appropriate supervisor, with reassessment for Level 1. Level 3 missed acknowledgement or assessment deadlines escalate to the service supervisor with documented interim protection. Level 4 overdue reviews or completion commitments escalate to the service manager. All levels increase immediately when risk increases.

A missed deadline remains recorded even after escalation. Reassignment, duplicate merging, or reopening does not reset the original clock. Staff may raise priority; clinical urgency may be lowered only by an authorized clinician after assessment and a documented reason. An authorized custody supervisor may lower operational urgency after verification. Technical personnel cannot downgrade clinical urgency. Repeat alerts may be linked to one incident, but suppression rules must not hide a new event, deterioration, or loss of signal.

Managing the alert service

A staffed response process will give every alert a named owner, backup coverage, and an auditable record. Software delivers and tracks alerts; designated people assess conditions, provide care or protection, and verify resolution. Pilot 100 will not launch until each shift has sufficient primary and backup coverage. An on-call arrangement must actually meet approved deadlines; being listed on a roster is insufficient.

Responsible role	Accountability
Pilot director	Overall performance, staffing readiness, unresolved failures, and corrective action.
Shift commander	Custody response, assignments, safe access, backups, and overdue operational alerts.

Responsible role	Accountability
Control-room officer	Monitors operational queue, dispatches responders, verifies acknowledgement, and escalates delays.
Clinical lead and designated clinical responder	Medical thresholds, triage, treatment, observation orders, and monitoring changes; coverage defined for every operating hour.
Education and case-management leads	Missed services, scheduling barriers, resident requests, and progression-record corrections.
Technology and security team	Assignments, batteries, connectivity, interfaces, cybersecurity, and verified recovery.
Independent oversight reviewer	Audits response evidence, privacy concerns, missed events, and reported performance.

Detection through verified closure

1. Create a record from a device, staff observation, resident request, tracking event, or service failure. Include source, original time, identity, location confidence, signal quality, proposed level, and relevant instructions.
2. Route to authorized personnel. Clinical details go to clinical staff; officers receive the location, urgency, and response instructions needed to assist. Level 1 triggers immediate emergency dispatch rather than an ordinary queue.
3. Assign a named responder. Acknowledgement means accepting responsibility, not merely opening the alert. Trigger backup channels when acknowledgement is absent.
4. Verify and act. Record dispatch, arrival, resident access, assessment, and intervention separately. Normal readings never override observed danger or a request for help.
5. Escalate delays or deterioration. Timers notify the accountable supervisor. Required protection and care continue during escalation.
6. Document findings, actions, notifications, and follow-up. An unresolved concern stays open with a named owner and due date.
7. Verify closure. Clinical disposition is authorized by clinical personnel; serious custody events receive supervisory review. Technical closure requires testing the restored function and addressing monitoring gaps. Closure does not cancel follow-up obligations.

Shift readiness, outages, and review

At handoff, custody and clinical leads review open urgent events, monitoring orders, required observations, outages, coverage gaps, and pending follow-up. Incoming personnel explicitly accept outstanding assignments. Confidential information is shared only with authorized roles.

Device personnel reconcile equipment and residents, inspect batteries and attachments, maintain spares, and document repairs. Control-room and clinical staff verify alert delivery to primary and backup

channels on approved schedules and after significant changes or failures. Drill loss of power, network, sensor coverage, alert delivery, and clinical availability before live use.

During outages, approved radios, direct observation, physical counts, and manual records provide continuity. Missing data displays as unavailable, never safe. Restore and test systems, then reconcile records using original event times. Cybersecurity containment must preserve essential care and safe manual operation. Recovery is not complete until service and safety checks pass.

Critical failures receive immediate review; supervisors review operations each shift. Clinical and operational teams examine patterns weekly; the pilot director reviews the complete scorecard monthly. Report acknowledgement, delivery, arrival, access, assessment, intervention, escalation, and closure by level. Show percentages within deadlines, medians, 90th percentiles, maximum delays, unanswered alerts, and missing timestamps. Include false and missed alerts, privacy incidents, resident concerns, required services delivered, and corrective-action owners and due dates. Averages cannot conceal serious delays.

Victims, families, officers, and community partners

Haven Alabama will remain victim-directed. Support will not require forgiveness, reconciliation, public disclosure, contact with the person who caused harm, or support for release. Notification and restorative-contact arrangements require appropriate authorization and respect for safety preferences.

Family Connect will provide only approved information. Families will not receive live tracking, private clinical records, or control over correctional decisions by default. Families can provide relevant concerns and practical support through documented channels.

Shield & Standards will separate confidential employee support from ordinary supervision and disciplinary records. Leadership can review staffing pressure, overtime, training, and safety trends without unrestricted access to private counseling content. Allegations against employees will receive fair investigation and correction procedures.

Covenant Connect will distinguish a referral from a confirmed service. A release plan is incomplete when housing is only a name on a list or an appointment has not been accepted. Vetted partners will receive only information needed for their assigned service.

Community repair will use approved eligibility, supervision, safety, and verified project records. Technology will help document contributions without authorizing exploitation or using a resident's labor as proof of rehabilitation by itself.

How information will move between systems

Each system retains responsibility for its authoritative records: custody information in the corrections management system; clinical care in clinical records; learning in the LMS; operational scans and movement in the tracking system; progression decisions in the authorized review record.

A controlled integration service will validate and exchange approved fields through supported interfaces. It will preserve the source, event time, receipt time, corrections, and verification status. It will reject or flag mismatched identities, duplicates, incomplete transfers, and stale information.

Every connection requires a written data specification, supported interface, responsible owner, security review, failure-handling plan, and acceptance test. Existing applications will not be assumed compatible because both use the internet. Tablet access and backend data exchange require separate verification.

Urgent clinical and custody response will continue without waiting for education or resident-app integrations. Direct, unsupported writes into a vendor database will not be a routine shortcut.

Alert exchanges and interface acceptance

Shared event identifiers link alerts and responses without copying sensitive health information into every system. Each connection requires agreed fields, a supported interface, an implementation quote, security review, failure handling, and acceptance tests. Shield & Standards may display operational summaries only after that function and interface are developed and tested; it is not an existing medical emergency system by assumption.

Resident requests need a visible receipt, honest service availability information, and immediate non-digital emergency alternatives. An AI tool will not be advertised as an emergency contact without staffed, tested emergency routing.

Privacy: connected services, limited access

ALPRP will require a documented purpose for each type of information collected. Collect only what is needed, limit access to legitimate duties, and avoid unnecessary duplication.

Detailed clinical information belongs in protected clinical systems. Responding officers receive enough information to act safely and promptly. Victim records, employee health records, resident journals, educational records, and custody records require distinct access rules.

People will receive understandable information about collection and use. Confidentiality will not be presented as absolute where emergency, safety, or legal duties require disclosure. Those limits will be explained before sensitive information is requested.

Resident tablets may be shared, inspected, lost, or replaced. Local browser storage alone will not be described as secure confidentiality. Production services require appropriate session protection, protected storage, sign-out, and recovery. A quick-exit button will not be represented as removing browsing history or eliminating access risks.

Public reporting will remove identifying and security-sensitive details and suppress small categories that could reveal a person. Aggregate reporting will not provide a public route to reconstruct private health or victim information.

Clinical privacy and accountable data governance

Before collecting health information, the implementing agency and clinical provider will identify who is responsible for it, which organizations are subject to HIPAA, and which suppliers act on their behalf. HIPAA applicability depends on the organization and activity; an app name or a prison location does not establish coverage.

Where required, vendors and their subcontractors will enter into appropriate Business Associate Agreements before receiving protected health information. These agreements will define permitted use,

safeguards, incident reporting, subcontractor responsibilities, access and correction support, and return or destruction at the end of service. A policy document is not a signed agreement or a compliance certification.

HIPAA permits specified disclosures in lawful custody settings for health, safety, and other authorized purposes. ALPRP will not promise an absolute ban that prevents necessary care or lawful disclosure. Each exception will have an authorized purpose, appropriate limits, and a reviewable record. Emergency access will be logged and reviewed. A disclosure exception is not permission for unrestricted browsing or general-purpose surveillance.

Data stewardship and vendor restrictions

Contracts will establish state control and designated clinical stewardship while preserving residents' applicable rights. Vendors and subcontractors may process or store records only to deliver specifically authorized services. They receive no independent right to sell, advertise with, profile people from, or train proprietary models on pilot information. Restrictions include raw records, derived information, and de-identified datasets; anonymization does not create permission for independent commercial reuse.

Apply these restrictions to subcontractors and any transfer of the service to a new owner. Require approved hosting and processing arrangements, access logging, audit rights, incident reporting, usable data export, contract termination assistance, and verified deletion of copies when retention authority ends. State ownership alone does not prevent misuse or establish privacy compliance.

A record-specific retention schedule will distinguish routine raw telemetry, clinically significant event data, clinical records, movement records, response logs, and complaints. Retain information only for a justified purpose or applicable requirement. Preserve evidence subject to incident investigation, legal holds, or other lawful obligations. Stage transitions will not automatically erase evidence. Deletion procedures must address active systems, caches, exports, and backup expiration, with documented verification. A universal thirty-day purge is not adopted by this framework. HIPAA does not itself establish a medical-record retention period; counsel and clinical records personnel must approve the applicable schedule. De-identification is permitted only for a specifically authorized continuing purpose, not as an alternative to deletion without justification.

Enforce separation across the whole ecosystem

Clinical-custodial data separation requires access controls, approved interfaces, audited disclosures, and tested exports, not merely different screens. Raw medical telemetry will not enter routine Saharah Compass guidance, the LMS, disciplinary records, or parole packets. Officers receive identity, location, urgency, and practical response instructions necessary to assist. Any exceptional disclosure requires a documented lawful basis and controlled access.

ALPRP prohibits using physiological anomalies, inferred emotions, or requests for care to generate disciplinary charges, progression penalties, or adverse parole recommendations. Lawfully compelled disclosures will be handled through authorized review; a policy restriction cannot promise immunity from legal process. Specific observed conduct remains subject to fair human review without treating biometric readings as proof of intent or guilt.

Victim-service records in Haven Alabama and confidential officer-support records require separate protections. Neither becomes a routine source of resident risk scoring or staff performance scoring.

Clinical information must not be sent to an external reviewer merely because an alert occurred; oversight receives the information authorized and necessary for its function.

Security: protect the whole service

The state-led technology team will establish security requirements before deployment. Access will depend on authenticated identity, authorized duties, and the minimum permissions needed.

Administrative access will require stronger protection, including multi-factor authentication for privileged and remote access. Any legacy limitation requires documented risk review and compensating controls before use.

Networks and services will be separated so that a resident-facing tablet cannot directly access custody databases, medical telemetry, officer alarms, or system administration. Sensitive information will be encrypted in storage and transmission using appropriate supported protections. No security claim will be applied to a radio link or device unless verified for that component.

Maintain device inventories, supported software, security updates, controlled vendor access, protected credentials, audit records, tested backups, and incident-response plans. Test recovery, not just backup creation. Security review will cover the applications, devices, networks, integrations, AI providers, and contractors together.

Staff and contractor entry controls will complement technology through approved screening, package procedures, reporting, and investigation. Tracking bracelets do not detect all contraband or establish its source.

Prototype applications will not receive real sensitive records until production security and governance are approved. Training and development will use synthetic or appropriately de-identified information.

Hosting and communications: prove security, not labels

The hosting environment will be selected through a documented assessment of the information, applicable requirements, operational needs, and supplier safeguards. HIPAA does not itself require a named government-cloud product. FedRAMP authorization or a SOC 2 report can inform review, but neither automatically makes the entire deployment compliant or safe. Verify the service, configuration, report scope, and responsibilities actually covered.

ALPRP will require documentation of where information is processed, who can access it, how encryption and keys are managed, and how service remains available. The review will include subcontractors and disaster-recovery arrangements. Encryption alone does not prevent unauthorized authorized-user access, false records, or outages.

Radio, Wi-Fi, and other connections will be evaluated against the intended use. ALPRP will not require one frequency band for every device or assume that a proprietary radio is impossible to intercept. Test coverage, interference, authentication, supported link protections, battery behavior, and recovery in the actual facility. Separate clinical and custody services where needed while allowing approved, tested exchanges.

Benefits and risks: what can go wrong, and what ALPRP will do

Intended benefit	What can go wrong	Prevention, correction, and improvement
Earlier awareness of physiological deterioration	Incorrect or missed readings can delay care; excessive alerts can overwhelm staff.	Validate the exact device, retain observation, assess symptoms, review false and missed alerts, and revise protocols under clinical direction.
Faster identity and movement verification	Misassigned devices, stale rosters, or failed scans can produce false accusations.	Verify assignments, reconcile rosters, show stale data, investigate discrepancies, correct records, and suspend consequential use of unreliable data.
Better documentation of checks	Staff may scan without observing or providing care.	Require appropriate observation records, audit checks against independent evidence, investigate false documentation, and improve supervision and training.
More education and treatment access	Device scarcity, disability barriers, outages, or lockdowns can deepen unequal access.	Measure actual access, provide accommodations and non-digital alternatives, repair faults, and reschedule missed services.
Supportive AI guidance	AI can give inaccurate advice, mishandle distress, or expose private information.	Limit its role, use approved content and providers, provide human escalation, protect data, review errors, and disable unsafe functions.
More coordinated records	A mistaken identity or flawed integration can spread incorrect information.	Use controlled matching, source labels, reconciliation, access limits, and traceable corrections that reach affected systems.
Stronger safety controls	Surveillance may become excessive or health data may be used to punish.	Limit purposes, restrict access, prohibit punitive biometric scoring, review necessity, and investigate misuse independently.
Better officer support	Wellness monitoring may discourage help-seeking if it feeds discipline.	Separate confidential support from supervision, explain disclosure limits, restrict access, and audit improper use.
More accessible victim services	Notifications or shared records may expose victims or create unwanted contact.	Respect preferences, separate records, verify recipients, correct notification errors, and enforce no-contact protections.

Intended benefit	What can go wrong	Prevention, correction, and improvement
Safe monitoring reduction and supported self-management	Premature removal, unnecessary continued collection, unsafe attachments, or loss of treatment can harm residents.	Require clinician-led review, separately authorize tracking, verify configuration changes, maintain observation and continuity, audit duration and removal delays, and review crises without automatic punishment.
More dependable technology	Outages, hacking, weak attachment design, or battery failure can create danger.	Test coverage and safety, monitor device health, maintain spares, practice manual fallback, isolate compromised equipment, and verify recovery.
Specialized contractor support	Vendor lock-in, hidden fees, or restricted exports can obstruct services and oversight.	Require usable exports, documented interfaces, state access, performance measures, transition assistance, and independently verified inventory.
Clearer public reporting	Attractive dashboards may hide missing data or exaggerate success.	Publish definitions, denominators, missing information, limitations, and failures; correct reports and seek independent verification.

These risks are real. Technology can amplify neglect when leaders treat equipment as a substitute for care, staffing, or accountability. ALPRP will evaluate whether each tool improves delivery in practice and will modify, suspend, or discontinue unsafe or ineffective functions.

Reporting concerns and correcting harm

Residents, families, victims, and staff need accessible ways to report inaccurate records, unmet needs, unsafe equipment, and misuse. Provide non-digital options and a protected route outside facility command for serious unresolved concerns. Explain who reviews a report, how urgent matters escalate, and how the person can follow up.

Reports will be logged and assessed without treating every allegation as an established fact. Retaliation concerns require protection review. Consequential decisions based on disputed technology records require human verification and appropriate correction or appeal procedures.

When harm occurs, preserve evidence; provide necessary care or protection; contain the technical or access failure; correct affected records; communicate with appropriate affected parties; and verify corrective action. Investigations will not be closed simply because equipment was restarted or a contractor marked a ticket resolved.

Confidential feedback and correction

Residents will have a confidential complaint route outside the ordinary custodial reporting chain, accessible without relying on a functioning tablet. Explain who receives complaints, how urgent concerns are escalated, and the limits of confidentiality. Prohibit retaliation for reporting harm, declining optional monitoring, requesting care, or disputing inaccurate records.

The designated reviewer will track complaints, response dates, remedies, and recurring patterns. Residents may request correction of inaccurate records through applicable procedures. Verified corrections must reach affected systems and decision-makers. Include resident feedback in pilot review, with safeguards against identification in public reports.

Procurement standards: evidence before expansion

Procurement will separate clinical monitoring, movement verification, education access, and application integration into clearly defined functions. A combined product can be considered when it safely meets those functions; an all-in-one promise will not replace evidence. Compare overlap so the state does not purchase duplicate services without a reason.

Readiness gate	Evidence required
Facility readiness	Survey of layout, power, network and radio coverage, installation needs, and staffing available to respond.
Clinical suitability	Approved monitoring review and discontinuation procedures, safe attachments and removal, care continuity, approved use cases, exact device and measurement documentation, relevant regulatory status, attachment assessment, contraindications, and clinician-led protocols.
Alert performance	Tested delivery, acknowledgement, escalation, missing-signal alerts, false and missed event review, and behavior under interruption.
Privacy and security	Approved access rules, required agreements, hosting assessment, documented safeguards, audit access, and tested recovery.
Integration	Supported field definitions and interfaces, identity matching, data freshness, correction handling, export, and outage reconciliation.
Human readiness	Demonstrated officer and clinical training, backup coverage, non-digital procedures, resident explanations, and accommodations.
Vendor accountability	Defined service obligations, repair and replacement arrangements, performance reporting, state access to records, and transition assistance.

Test in a limited operational area before expansion. The pilot can use documented internal thirty-, sixty-, and ninety-day implementation checkpoints where appropriate; these are distinct from the public reporting schedule; elapsed time alone will not establish readiness. Essential identity and clinical integrations must be tested before live use when the workflow depends on them. Broader reporting connections can follow after acceptance. A blanket ninety-day ban on all integrations could itself create unsafe duplication and identification errors.

Independent clinical and technical reviewers will receive enough documentation to evaluate measurement accuracy, notification logic, known limitations, and changes. Vendors must demonstrate performance across relevant residents and operating conditions. A proprietary algorithm or an individual baseline will not be accepted as proof that bias has been resolved.

Vendor updates that affect readings, alerts, security, or interfaces require change review and appropriate retesting. Serious recurring failures can trigger restricted use, suspension, repair, or replacement. Clinical services and required observation continue during those actions. Payment and expansion milestones will depend on accepted deliverables, not installation alone.

Implementation and oversight

ALPRP proposes that Alabama lead the model through accountable corrections, clinical, education, reentry, and technology personnel. Contractors may supply specialized equipment and services. Public responsibility will remain with the agency authorizing and operating the program.

Start with limited, supervised use. Expand only after acceptance testing. Review performance at 30, 90, 180, and 365 days following operational launch. These are proposed review points, not promises about launch dates or clinical outcomes.

Launch, suspension, and restart authority

Before live use, the pilot director, clinical lead, custody lead, and technology/security lead must document readiness for their responsibilities. Test every shift, simultaneous emergencies, access to locked areas, signal loss, identity mismatches, duplicate-alert suppression, outages, and backup dispatch. Do not activate a function whose necessary response coverage or interface is unproven.

Trigger	Immediate protection	Accountability and restart
Missed critical alert, unsafe delay, or observation gap	Restore required human protection; assess the resident; dispatch backup and clinical help as needed.	Preserve evidence; identify cause and corrective action; test the response pathway before restoring an unsafe function.
Serious skin injury or unsafe attachment	Remove or adjust as clinically indicated; provide alternative protection.	Clinical lead reviews the resident and model; verify suitability before reuse.
Excessive alarms, hidden deterioration, or unreliable identity/location	Maintain direct checks and manual verification; isolate the unreliable function.	Review missed events as well as false alerts; validate changes under realistic conditions.
Unauthorized disclosure or compromised records	Contain access and maintain safe care through approved alternatives.	Security and privacy leads investigate, follow applicable notification duties, and verify recovery.
Insufficient staffing or backup coverage	Maintain required care and observation; do not rely on the affected monitoring function.	Pilot leadership restores demonstrable response capacity before resumption.

Qualified clinicians may order immediate device removal or changes to clinical monitoring when necessary for safety. Custody and security leads may isolate unsafe operational or technical functions within their authority. All staff can activate emergency protection and report unsafe conditions. The pilot director will ensure that suspension decisions and unresolved risks reach the designated independent reviewer.

A missed critical response deadline creates an escalation and review record, not an automatic finding of misconduct. RF proximity does not prove assessment or care. An external oversight recipient, authority, secure reporting route, and review arrangements must be established before launch; this framework does not assume an existing twenty-four-hour ombudsman service.

Restart requires evidence that the cause was addressed, the corrected function was tested, and appropriate clinical, operational, and technical leaders approve resumption. Independent review will examine serious failures and recurring patterns. Expansion requires demonstrated safe delivery, not merely vendor assurances or elapsed time.

Pilot 100: tracking, discipline, behavior, and public-value KPIs

Pilot 100 will use a defined scorecard to evaluate safety, treatment access, reliable operations, fair accountability, learning, and fiscal viability. A KPI is a key performance indicator: a measurement with a clear definition, reliable source, responsible reviewer, and published limitation. Purchasing wearables will not establish that the pilot works.

Establish the baseline before making claims

The baseline column will read "to be established" until ADOC supplies and validates the relevant records. ALPRP will not label response times, hospital use, false alarms, or suicide-watch hours as an ADOC average without evidence.

Use the pilot unit's preceding 12 months for routine operational comparisons and, where available, three years for rare severe events. Preserve monthly values rather than combining all history into an unexplained average. Report layout, staffing, occupancy, clinical needs, lockdowns, and policy changes. Where feasible, use a comparable non-pilot unit and review differences in population and services. Pilot enrollment, withdrawals, transfers, and device eligibility will be documented to prevent selection of only easier cases.

Rates for events will use resident-days: one resident present for one day equals one resident-day. Report events per 1,000 resident-days, raw counts, severity, and the number of affected people. Report clinician-monitored days separately. A 100-person pilot may not establish a statistically reliable reduction in rare deaths or severe self-harm. Evaluation will include uncertainty intervals and independent review; a before-and-after improvement alone does not prove technology caused it.

Life safety and clinical care

Indicator	Definition and verification	Proposed Year 1 goal
Severe self-harm and suicide outcomes	Separate counts and rates of suicide deaths, attempts, and clinically defined severe injuries; reconcile clinical records, incident reports, and outside-hospital records. Clinical leadership reviews every severe event and near miss.	Aim to reduce harm. A 50% reduction may be stated as an exploratory aspiration after baseline review, never a guaranteed minimum or evidence of lives saved.
Earlier recognition of suspected overdose or deterioration	Count clinician-reviewed episodes where a wearable alert preceded documented staff recognition; record the time difference, actual intervention, and outcome. Identify how many confirmed events had no useful alert.	Improve recognition and timely appropriate care; assess missed events as well as successful alerts. No claim that an alert proves an overdose or prevents ICU admission.
Time to clinical assessment	Measure alert generation to clinical acknowledgement, physical assessment, and appropriate treatment separately; report median, 90th percentile, maximum, and overdue cases by urgency.	Meet clinician-approved urgency-specific deadlines. Emergencies receive immediate response; routine mental-health checks do not replace emergency care.
Observation and treatment delivered	Completed required direct observations divided by observations due; clinically ordered treatment delivered divided by treatment due, with omissions and reasons. Verify through clinical orders, staff records, and independent audits.	100% of required observation and treatment obligations met; investigate every omission. No target to eliminate suicide-watch staff hours.
Clinical follow-up and continuity	Alerts with documented disposition and follow-up divided by alerts requiring follow-up; review treatment handoffs after moves and release.	100% of urgent events assigned and reviewed; close only after verified action and required follow-up.

Medical thresholds will be selected by licensed clinical leadership for the exact validated device, intended use, individual condition, and approved response protocol. ALPRP will not adopt oxygen saturation below 85% as a universal first-alert threshold or wait for that level before responding to deterioration. Heart-rate variability and pacing do not independently establish a psychiatric crisis, aggression, or suicidal intent. Device accuracy, signal quality, symptoms, medications, and missing data must be considered. FDA information identifies accuracy limitations in pulse oximetry, including concerns related to skin pigmentation.

Tracking, device reliability, and staff response

Indicator	Definition and verification	Proposed Year 1 goal
Identity assignment accuracy	Correct resident-device assignments divided by audited assignments; verify against the authorized roster, photograph, and physical identification.	100% correct before operational use; immediately correct and review every mismatch.
Tracking availability and location accuracy	Valid, sufficiently fresh monitored-zone minutes divided by required monitoring minutes; separately compare zone reports with independently observed location. Include battery, network, and sensor outages.	Candidate availability target of at least 99% during required monitoring; prove site-specific zone accuracy before use. Targets require acceptance testing and manual fallback at every outage.
Physical-count reconciliation	Counts completed under approved procedure; number and duration of discrepancies; distinguish device errors from confirmed missing residents.	100% of required physical counts retained; reconcile every discrepancy without relying solely on a device signal.
Movement and separation events	Confirmed unauthorized movements or separation-plan breaches per 1,000 resident-days; report false alerts, authorized exceptions, and time to verification separately.	Reduce confirmed breaches without unnecessary restrictions or false allegations; set the numerical improvement goal after baseline validation.
Battery and device management	Scheduled inspections completed; low-battery alerts resolved before loss of coverage; unavailable hours, replacement time, attachment problems, and repair recurrence.	100% of required inspections; resolve battery warnings within a tested maintenance window; no unassigned monitoring outage.
Emergency response latency	Measure event generation, delivery, acknowledgement, arrival of the first qualified responder, required response-team arrival, resident access, and start of care. Use synchronized clocks and verified incident records.	Proposed arrival goal below 180 seconds, subject to approved emergency protocols and site drills. It is a performance ceiling for evaluation, never permission to wait three minutes. Report the percentage meeting it and all exceptions.
Welfare-check verification	Checks with evidence of the required observation divided by checks due. Report RF or scan agreement as a separate corroboration measure and independently audit a sample.	100% of required checks completed; investigate missing checks and scan-without-observation cases. RF proximity cannot prove face-to-face observation, meaningful contact, or care.
Alert usefulness and missed events	Clinician- or supervisor-adjudicated actionable alerts divided by reviewed alerts; separately report false alerts per 100 monitored hours, missed confirmed events, and unknown classifications.	Candidate custodial alert precision above 90% only after validation, while preserving sensitivity to serious events. Thresholds cannot be adjusted merely to improve this percentage.

The percentage of alerts routed to clinicians versus custody is a routing measure, not a true-positive rate. Custody receives the location, urgency, and actions needed to assist; clinical staff retain detailed health information. Each alert type needs its own denominator, independent event review, and definition of "actionable." A low false-alert percentage can conceal dangerous missed events. Include signal loss, delayed delivery, duplicate alerts, and events found by staff without a wearable alert.

The approved emergency system will be the source for operational timestamps. Shield & Standards may display authorized summaries through a tested interface; its conceptual dashboard will not be presented as an existing medical alert system. Guard1, the corrections management system, and clinical systems remain distinct sources until interfaces and capabilities are verified.

Discipline, observed behavior, education, and progression

ALPRP will document specific observable conduct, context, and verified achievements. Residents will receive understandable expectations, access to records appropriate to their rights, a correction process, and human review. Seeking help, reporting harm, disability-related behavior, or a clinical symptom will not become an automated misconduct score. Biometric data, AI emotion predictions, and device proximity alone will not determine guilt or stage progression.

Indicator	Definition and verification	Proposed Year 1 goal
Serious violence and victimization	Confirmed assaults and injuries by severity per 1,000 resident-days; reconcile incident reports, medical findings, and confidential reporting. Track resident and officer harm separately.	Reduce harm; set a percentage target after baseline review. Increased reporting will be analyzed rather than automatically labeled worsening behavior.
Disciplinary cases and repeat violations	Report allegations, cases resolved, sustained findings by severity, and residents with repeat sustained violations within a defined 90-day follow-up window. Use decisions and appeal results, not raw device alerts.	Reduce serious and repeated sustained violations; report pending cases and follow-up time. No quota to write fewer reports or suppress complaints.
Fair disciplinary review	Cases with required notice, evidence review, accommodations, decision reasons, and available appeal procedures divided by cases due; report reversals and correction delays.	100% of required safeguards; correct overturned findings in all affected progression records.
De-escalation and restrictive interventions	Episodes resolved safely using documented de-escalation; separately track force, restraints, restrictive housing days, injuries, and subsequent escalation. Audit incident severity and classification.	Improve safe resolution and reduce avoidable restriction without discouraging necessary emergency protection. Clinical distress prompts assessment.

Indicator	Definition and verification	Proposed Year 1 goal
Positive behavior and responsibility	Verified completion of individualized commitments, safe work, conflict-resolution practice, approved mentoring, and restorative activities. Supervisors document evidence and opportunities available.	Set attainable individual goals and verify achievement. Do not penalize residents for unavailable opportunities or require victim participation or forgiveness.
Education access and achievement	Attended sessions divided by accessible scheduled sessions; instructor-confirmed competencies, course completion, and credentials. Also report all scheduled sessions and cancellations.	Improve verified learning; reschedule missed access. Attendance, tablet use, or Compass engagement alone is not mastery.
Treatment participation and service barriers	Treatment offered, attended, clinically adjusted, declined, or prevented; distinguish informed choices from escort failures, outages, lockdowns, and accommodations not provided.	Deliver the approved care plan and remedy barriers. Do not treat symptom-related inability or technology failure as automatic noncompliance.
Progression review and readiness	Reviews held when due; decisions with verified education, treatment summaries authorized for sharing, work evidence, reasons, and correction records.	100% of due reviews completed and decisions explained; no automated stage advancement, denial, or parole recommendation.

Behavior measures will be reviewed for consistency between officers and shifts and for unequal application. Use authorized, protected subgroup analysis to identify differences by clinical need, disability, race, stage, housing, and access to services where lawful and statistically meaningful. Small groups will be protected from identification in public reporting. Do not rank units or residents using an opaque combined "good behavior" score.

Fiscal viability without reducing required care

Fiscal evaluation will measure actual resource use and documented costs, while maintaining this framework's no-budget format. Finance personnel will reconcile clinical utilization with invoices, payroll, transport records, vendor charges, and implementation records.

- Track external emergency visits, hospital admissions, ICU use, transports, and inpatient days per 1,000 resident-days, separated by acuity and clinical indication. A proposed 35% reduction in external transports is an exploratory goal to assess after baseline review, not a restriction on transfers or a guaranteed saving. Monitor delayed transfers, deterioration, readmissions, and clinical outcomes as balancing measures. A clinician decides whether infirmary care is appropriate.
- Measure overtime, required observation staffing, alert-response time, administrative time, escorts, training, and maintenance separately. Efficiency gains may come from scheduling, reconciliation, and fewer duplicate administrative tasks. Continuous wearables and periodic rounds will not replace prescribed continuous observation. Changing observation level requires clinical assessment and approved procedures, not a cost target.

- Calculate net pilot cost as implementation and operating costs plus additional clinical, technology, and response staffing, minus verified cash expenditures actually avoided. Include equipment, replacements, infrastructure, licenses, interfaces, security review, training, maintenance, and independent evaluation. Separate cash savings from staff time redeployed and projected future cost avoidance. Avoid double-counting transport or payroll costs already included in another category.
- Report cost per resident-day and cost per verified service delivered, alongside safety and access measures. Compare compatible periods and account for census, acuity, staffing, price changes, and the cost of providing services previously missing.
- Track actual legal-defense expenditures, claims, settlements, and substantiated rights violations as context. Do not assign a dollar value to "avoided litigation" or infer savings from fewer incidents alone. Small-pilot results cannot establish how many lawsuits or deaths would otherwise have occurred.

Fiscal viability means demonstrable value and sustainable delivery within approved resources. It does not mean a requirement that Pilot 100 produce immediate cash savings. Earlier identification may appropriately increase assessment or hospital use during initial implementation.

Who reviews the scorecard, and when

Clinical leadership owns clinical definitions, thresholds, event adjudication, and care safeguards. The pilot operations lead owns movement, rounds, counts, response staffing, and drills. Education staff verify learning. Human decision-makers verify discipline and progression. The technology team verifies uptime, matching, clocks, integrations, and logs. Finance validates costs. An independent evaluator checks methods, missing data, and claims; privacy and security personnel control access and disclosure.

Before launch, approve a metric dictionary with the numerator, denominator, exclusions, source system, timestamp rules, owner, target, and correction process for every KPI. Validate retrospective baseline records and acceptance-test the new measurements. Any comparison target that remains unsupported will be labeled provisional.

Review urgent failures immediately, shift readiness at each handoff, operational patterns weekly, and the complete scorecard monthly. Publish reviewed aggregate findings at 30, 90, 180, and 365 days after launch. Each report will state counts, rates, missing records, unavailable monitoring time, changes in definitions, target status, and corrective actions. Retain original records and traceable corrections. Do not remove inconvenient incidents or classify missing signals as normal readings.

Evaluation that separates technology from better services

Where feasible, compare Pilot 100 with a unit receiving similar improvements in staffing, rounds, and treatment without the same wearable intervention. Document differences and recognize when a suitable comparison is unavailable. Evaluate the additional benefit of wearables rather than attributing every improvement to equipment.

Report consent and withdrawal patterns, alternative-care access, device injuries, complaints and remedies, missed emergencies, required observations, service delivery, and resident-reported safety alongside existing clinical, operational, educational, and fiscal KPIs. Independently review whether alarm suppression or threshold changes hide deterioration. Protect small groups in public reporting.

Civil-liberties commentary identifies concerns and ethical objections; investigative journalism documents experiences and failures; conceptual engineering papers suggest architecture; vendor materials describe claimed capabilities. None alone establishes clinical effectiveness. Product-specific evidence, site testing, and independently reviewed pilot outcomes are required. ALPRP will describe wearable benefits as potential until supported and will publish findings that do not favor expansion.

Supporting references

Sources checked October 5, 2026. Official guidance informs safeguards; vendor pages describe claimed product capabilities; civil-liberties commentary and journalism identify concerns; the engineering paper is conceptual. Proposed pilot targets are ALPRP proposals rather than requirements established by these sources. These references describe product capabilities or relevant safeguards. They do not establish that ALPRP has been adopted, that the proposed systems are integrated, or that clinical outcomes are guaranteed.

- [ALPRP proposed applications](#)
- [ALPRP systemwide safeguards](#)
- [ALPRP victim support](#)
- [ALPRP officer support](#)
- [Guard1 tracking and verification](#)
- [Guard1 integrations](#)
- [OverWatch vendor description](#)
- [Biobeat current product information; exact model and intended use require verification](#)
- [FDA pulse oximeter information](#)
- [NIST supplier-risk guidance](#)
- [HHS HIPAA and cloud computing guidance](#)
- [HHS guidance on disclosures to law enforcement and correctional institutions](#)
- [HHS medical-record retention guidance](#)
- [NIST digital authentication guidance and non-biometric alternatives](#)
- [ACLU analysis of biometric bracelets and staffing concerns](#)
- [The Marshall Project reporting on biometric bracelets](#)
- [Conceptual IoT tracking paper; not evidence of clinical effectiveness](#)
- [FDA biocompatibility evaluation by contact duration](#)