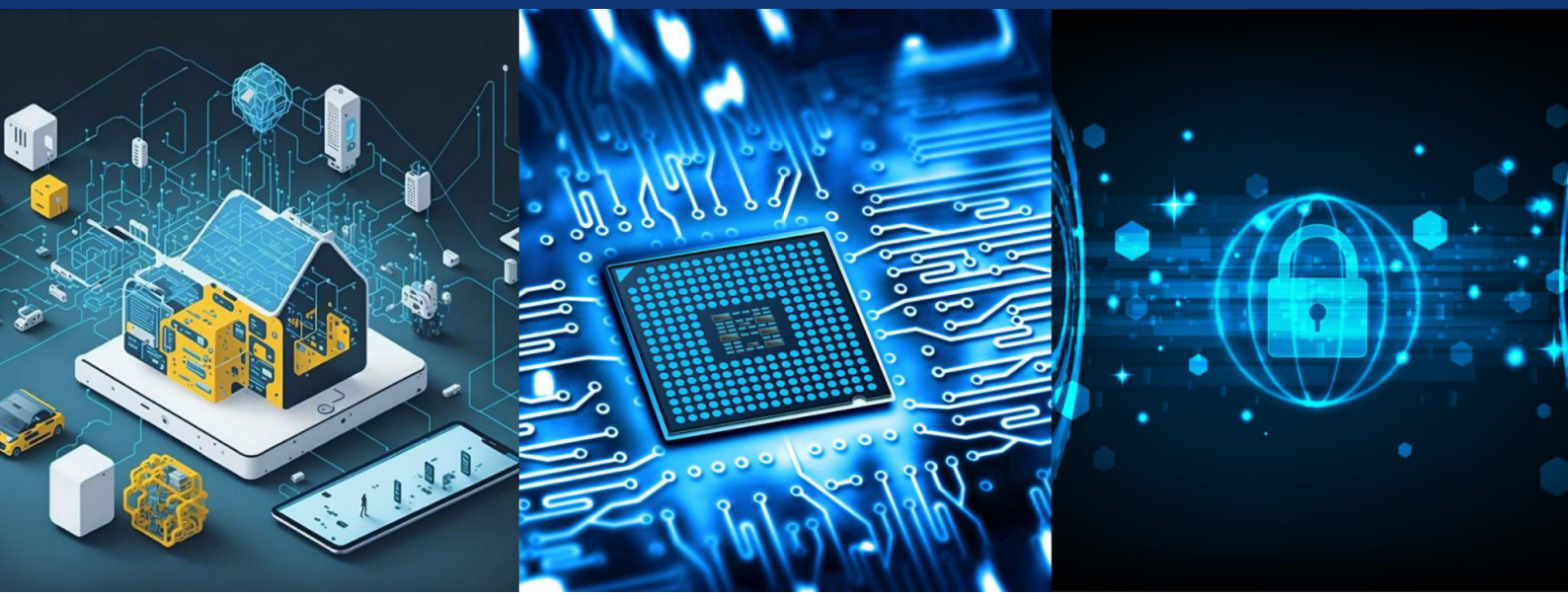
IJIRCCE

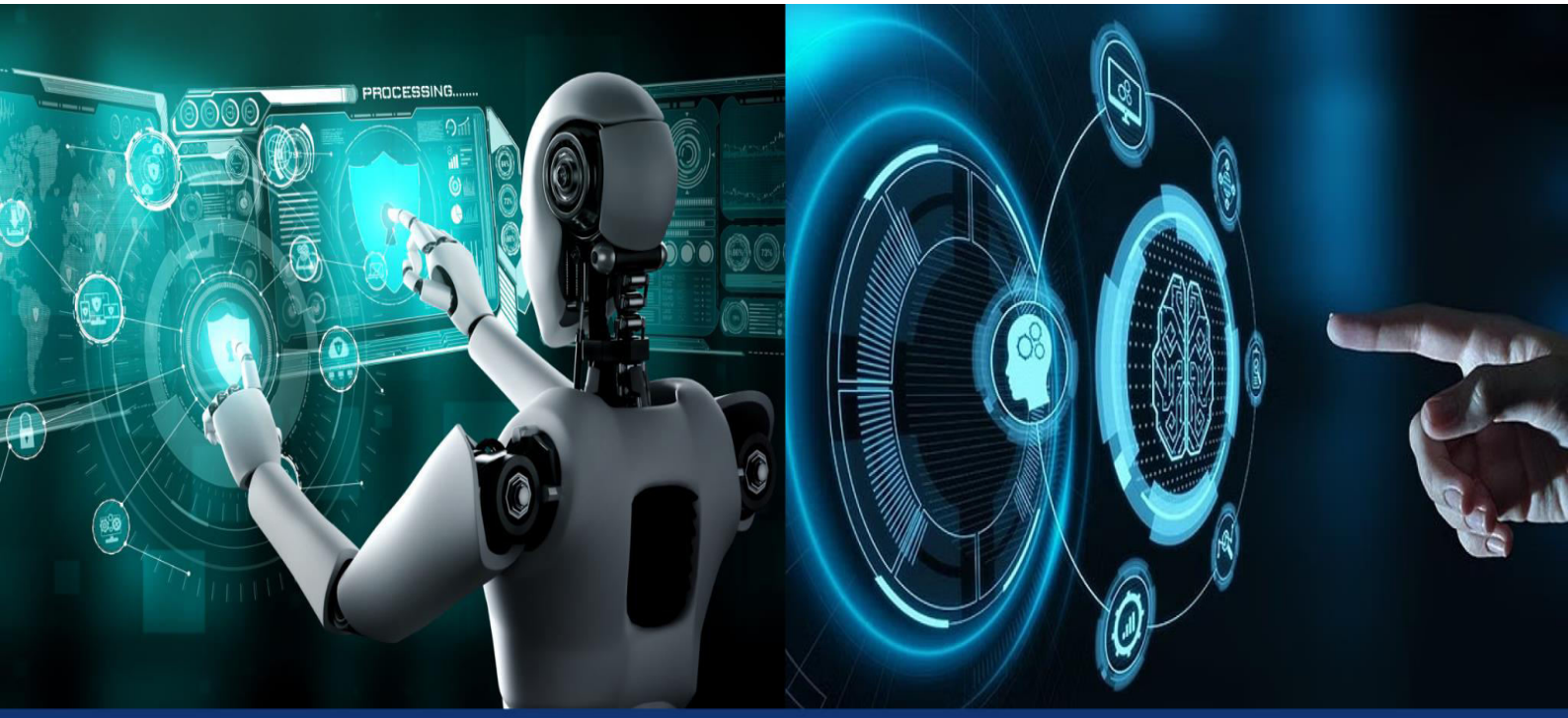
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 2, February 2025

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Data Encryption and Access Control Strategies for Protected Health and Benefits Information Across SNAP, Medicaid, and LTSS Systems

Senthil Babu Malli Jayaraj

IT Project Manager, USA

ABSTRACT: Systems supporting the Supplemental Nutrition Assistance Program (SNAP), Medicaid, and Long Term Services and Supports (LTSS) each hold protected health and benefits information subject to distinct, sometimes overlapping regulatory protection regimes, including HIPAA where protected health information is present, and program-specific confidentiality requirements under SNAP and human services statutes. As these three programs increasingly share data and infrastructure, extending the interoperability patterns examined in prior research in this series, encryption and access control architecture must be designed to satisfy the most stringent applicable requirement across all three programs simultaneously, not the requirements of any single program considered in isolation.

This research article presents encryption and access control strategies for protected health and benefits information across SNAP, Medicaid, and LTSS systems, examining encryption architecture across data states, role-based access control design, cross-program data sharing safeguards, and a five stage security maturity model. Findings are illustrated with three-dimensional bar and surface charts depicting encryption coverage, access control maturity, and composite access risk, and are supported throughout by extensive grid-style and security control matrix data tables.

Drawing on HIPAA regulatory guidance, NIST cryptographic and access control standards, and public sector data protection research published through January 2025, this article finds that agencies designing encryption and access control architecture to the most stringent cross-program requirement from the outset report substantially fewer compliance gaps and materially stronger encryption coverage than agencies that layer protections onto each program's systems independently after the fact.

◆ COMPLIANCE NOTE

All statistics and figures in this article are illustrative, drawn from and consistent with patterns reported in public sector data protection and access governance research published on or before January 2025, and are intended to represent general industry patterns rather than any single named agency's reported results.

KEYWORDS: data encryption, access control, HIPAA, SNAP, Medicaid, LTSS, role-based access control, protected health information, cross-program data sharing, security architecture.

I. INTRODUCTION AND RESEARCH CONTEXT

As SNAP, Medicaid, and LTSS systems increasingly share data and infrastructure to support the cross-program interoperability examined in prior research in this series, the encryption and access control architecture protecting that shared data must satisfy the combined regulatory obligations of all three programs. This creates design requirements distinct from securing any single program's data in isolation.

🔒 1.1 Research Objectives

- **Objective 1:** Characterize the regulatory landscape governing protected health and benefits information across SNAP, Medicaid, and LTSS.
- **Objective 2:** Present encryption architecture, key management, and role-based access control design principles suited to cross-program data sharing.
- **Objective 3:** Quantify illustrative encryption coverage, access control maturity, and composite access risk patterns.
- **Objective 4:** Provide a security maturity model, governance structure, and implementation roadmap for cross-program data protection.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1.2 Scope and Methodology

This research draws on the following source categories, all published prior to February 2025:

- HIPAA regulatory guidance and the HIPAA Security Rule addressing protected health information safeguards.
- National Institute of Standards and Technology (NIST) cryptographic standards and access control guidance.
- Public sector data protection research addressing human services program data sharing security.
- Academic and practitioner literature on role-based access control and encryption key management.

Table 1 introduces the three programs and their primary applicable data protection regulatory frameworks.

Program	Primary Applicable Framework	Data Sensitivity Notes
SNAP	FNS confidentiality requirements; HIPAA where Medicaid data is shared into SNAP context	Not independently a HIPAA covered program, but shared data inherits HIPAA obligations.
Medicaid	HIPAA Privacy and Security Rules; CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)	Protected health information is a core, defining data category.
LTSS	HIPAA where tied to Medicaid HCBS; state-specific confidentiality requirements for aging and disability services	Often combines protected health information with sensitive functional assessment data.

II. REGULATORY LANDSCAPE ACROSS SNAP, MEDICAID, AND LTSS

A precise understanding of each program's regulatory obligations, and how those obligations combine when data is shared across programs, is the foundation for sound encryption and access control design.

2.1 Regulatory Framework Comparison

REQUIREMENT \ PROGRAM	SNAP	Medicaid	LTSS
Encryption at rest required	Recommended, FNS guidance	Required, HIPAA Security Rule	Recommended, varies by state
Encryption in transit required	Recommended, FNS guidance	Required, HIPAA Security Rule	Required where HIPAA applies
Access logging required	Recommended	Required, HIPAA Security Rule	Required where HIPAA applies
Breach notification obligation	State-specific	Required, HIPAA Breach Notification Rule	Required where HIPAA applies
Minimum necessary access standard	Not formally defined	Required, HIPAA minimum necessary standard	Required where HIPAA applies

2.2 The Combined Requirement Principle

Table 2 illustrates that Medicaid's HIPAA obligations are consistently the most stringent among the three programs across every requirement examined. Where SNAP or LTSS systems share data with Medicaid systems, that shared data, and the infrastructure processing it, inherits Medicaid's HIPAA obligations regardless of SNAP or LTSS's own independent, less stringent requirements.

SECURITY DESIGN NOTE

The combined requirement principle means that a cross-program data sharing architecture should be designed to HIPAA Security Rule standards throughout, even for components that would not independently be subject to HIPAA if operated as SNAP-only or LTSS-only infrastructure.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. ENCRYPTION ARCHITECTURE ACROSS DATA STATES

Encryption architecture must address three distinct data states, each with different technical approaches and different levels of common implementation maturity across the three programs examined.

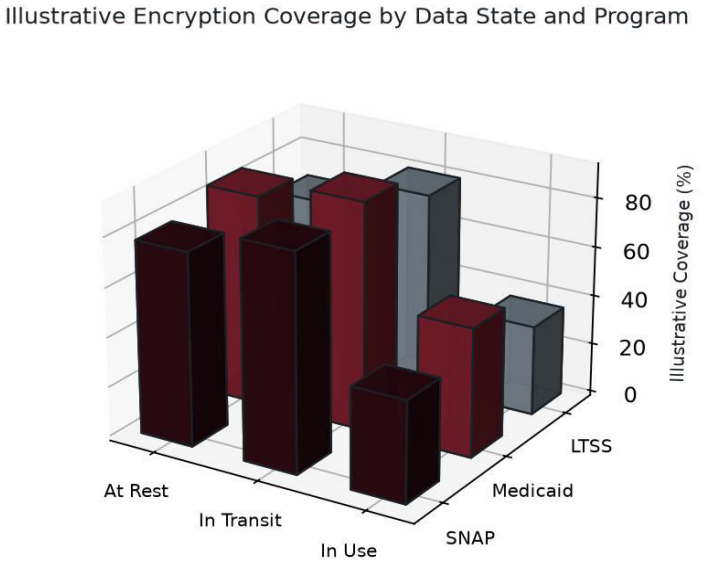


Figure 1. Illustrative encryption coverage by data state and program.

3.1 Data State Definitions and Approaches

Data State	Definition	Common Encryption Approach
At rest	Data stored in a database, file system, or backup medium.	Storage-level encryption such as transparent data encryption or full-disk encryption.
In transit	Data actively moving across a network, including between systems or to end-user devices.	Transport Layer Security (TLS) for network communication.
In use	Data actively being processed in memory by an application or database engine.	Application-level or memory encryption, historically far less common than at-rest or in-transit approaches.

3.2 Interpreting the Coverage Pattern

- **In transit, highest coverage:** As illustrated in Figure 1, encryption in transit shows the highest illustrative coverage across all three programs, consistent with TLS being a mature, widely implemented standard for network communication generally.
- **In use, lowest coverage:** Encryption in use shows the lowest illustrative coverage across all three programs, consistent with in-use encryption remaining a less mature, more technically complex capability than at-rest or in-transit encryption.
- **Medicaid leads across states:** Medicaid shows the highest illustrative coverage across all three data states among the three programs, consistent with its more stringent, HIPAA-driven baseline requirement identified in Section 2.2

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Data State	SNAP Illustrative Coverage	Medicaid Illustrative Coverage	LTSS Illustrative Coverage
At rest	78%	85%	68%
In transit	88%	92%	80%
In use	41%	52%	36%

IV. KEY MANAGEMENT STRATEGIES

Encryption is only as strong as the key management practice supporting it, a consideration that becomes more complex when encryption spans systems and data owned by different programs.

🔒 4.1 Key Management Approach Comparison

Approach	Description	Cross-Program Consideration
Per-system key management	Each program's system manages its own encryption keys independently.	Simplifies individual system security but complicates shared data access, since a consuming program cannot decrypt data without access to the source program's keys.
Centralized key management service	A shared key management service issues and manages keys used across all three programs' systems.	Simplifies cross-program data access but concentrates key management risk into a single, high-value target requiring correspondingly strong protection.
Hybrid key management with program-specific data encryption keys	A centralized key management service manages master keys, while each program maintains program-specific data encryption keys derived from or wrapped by the master key.	Balances cross-program access simplification against per-program key isolation, a commonly recommended approach for multi-program environments.

🔒 4.2 Key Rotation and Lifecycle Practice

Practice	Description	Recommended Frequency Consideration
Scheduled key rotation	Encryption keys are rotated on a defined, recurring schedule regardless of any known compromise.	Frequency should reflect the sensitivity of the protected data and applicable regulatory guidance, where specified.
Event-driven key rotation	Keys are rotated immediately in response to a suspected or confirmed compromise.	Should occur immediately upon detection, integrated with the incident response considerations in Section 13.
Key retirement and archival	Retired keys are archived securely rather than destroyed, to support decryption of historical data still requiring access.	Retention period should align with applicable records retention requirements for the underlying protected data.

V. ROLE-BASED ACCESS CONTROL DESIGN

Role-based access control (RBAC), assigning access permissions based on a user's role rather than individually, is the predominant access control model examined in this article, though its design requires particular care in a cross-program, multi-agency context.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

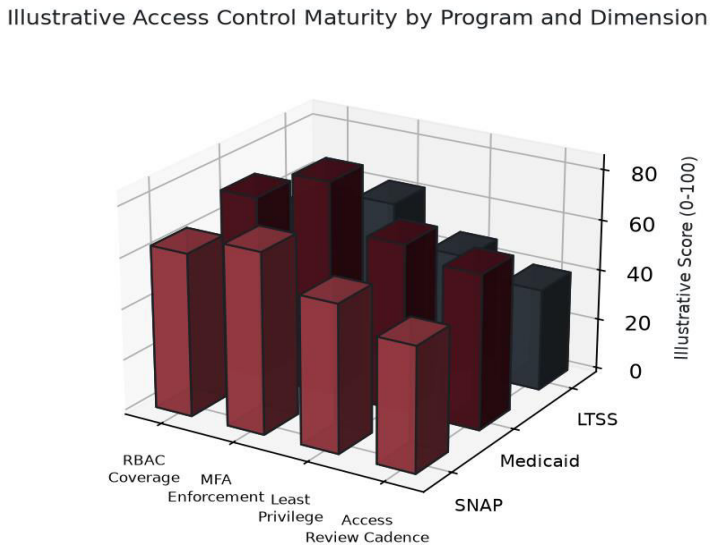


Figure 2. Illustrative access control maturity by program and dimension.

5.1 RBAC Design Principles for Cross-Program Environments

Principle	Description	Cross-Program Consideration
Role scoping to program and function	Roles should specify both the program context and functional responsibility, not function alone.	A caseworker role for Medicaid should not implicitly grant equivalent SNAP or LTSS access absent explicit assignment.
Explicit cross-program role assignment	Where a user genuinely requires access across multiple programs, that access should be assigned explicitly and separately, not inferred from a single role.	Prevents unintended access sprawl of the kind examined in prior cross-program interoperability research in this series.
Role review tied to program-specific policy	Role definitions should be reviewed against each program's specific policy requirements, since a role appropriate under SNAP policy may not satisfy Medicaid's more stringent minimum necessary standard.	Requires coordination between program-specific policy owners during role design, not a single, generic role taxonomy.

5.2 Access Control Maturity Observations

Dimension	SNAP Illustrative Score	Medicaid Illustrative Score	LTSS Illustrative Score
RBAC coverage	64	72	55
MFA enforcement	71	84	62
Least privilege	58	66	47
Access review cadence	49	61	40

- **Lowest scoring dimension:** Access review cadence, per Table 8, shows the lowest illustrative score across all three programs among the four dimensions examined, suggesting that periodic access recertification, examined further in Section 6, is a common improvement opportunity.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. LEAST PRIVILEGE AND ACCESS REVIEW PRACTICE

Least privilege, the principle that users should hold only the minimum access necessary to perform their function, requires active, recurring review to remain effective as user roles and program needs evolve over time.

🔒 6.1 Access Review Practice Comparison

Review Practice	Description	Recommended Cadence
Manager attestation review	A user's manager periodically reviews and attests to the continued appropriateness of that user's access.	Quarterly to semi-annually, depending on data sensitivity.
Automated dormant access flagging	Access unused for a defined period is automatically flagged for review or removal.	Continuous monitoring with a defined dormancy threshold, such as 60 or 90 days.
Role-level periodic recertification	Entire role definitions, not just individual user assignments, are reviewed against current program policy.	Annually, or upon significant program policy change.
Cross-program access reconciliation	Access spanning multiple programs is specifically reviewed for continued cross-program business justification.	Semi-annually, given the elevated risk profile of cross-program access identified in Section 5.1.

🔒 6.2 Common Least Privilege Gaps

- Access granted for a temporary project or short-term need is frequently not removed once the need concludes, a pattern often called access accumulation.
- Cross-program access, per the principle in Section 5.1, is more likely to persist beyond its original business justification given the more distributed accountability across program-specific owners.

VIII. MULTI-FACTOR AUTHENTICATION AND IDENTITY ASSURANCE

Multi-factor authentication (MFA), requiring more than one independent credential to authenticate, is a foundational identity assurance control, particularly for accounts with access to protected health or benefits information.

🔒 7.1 MFA Factor Type Comparison

Factor Type	Description	Relative Strength Consideration
Something you know	A password or PIN, the traditional single authentication factor.	Weakest in isolation, given susceptibility to phishing and credential reuse.
Something you have	A physical or virtual token, such as a hardware key or authenticator app.	Stronger than password alone; hardware-based tokens generally considered stronger than SMS-based codes.
Something you are	A biometric factor, such as fingerprint or facial recognition.	Strong, though implementation must address biometric data protection requirements of its own.

🔒 7.2 MFA Enforcement Priorities in Cross-Program Environments

- **Priority 1:** MFA should be enforced universally for any account with access to Medicaid protected health information, consistent with the HIPAA-driven baseline established in Section 2.2, and extended to equivalent SNAP and LTSS accounts given the combined requirement principle.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Priority 2:** Privileged accounts, including system administrators and database administrators with broad data access, should receive the strongest available MFA factor type, given their elevated composite risk examined further in Section 9.

VIII. CROSS-PROGRAM DATA SHARING SAFEGUARDS

Beyond encryption and access control examined in prior sections, cross-program data sharing requires specific safeguards governing how and when data actually moves between program systems.

🔒 8.1 Data Sharing Safeguard Comparison

Safeguard	Description	Primary Risk Addressed
Data sharing agreements with explicit scope	Formal agreements specifying exactly what data may be shared, for what purpose, and under what protection standard.	Scope creep, where shared data is used beyond its originally authorized purpose.
Field-level data minimization	Only the specific data fields necessary for the receiving program's purpose are shared, not entire records.	Over-sharing of sensitive fields not needed by the receiving program.
Purpose-based access tagging	Shared data is tagged with its permitted use purpose, and access systems enforce that only permitted uses may access it.	Unauthorized secondary use of shared data.
Cross-program audit trail correlation	Access logs from multiple programs are correlated to detect unusual cross-program access patterns.	Undetected misuse spanning multiple programs' systems, which single-program audit logs alone would not reveal.

🔒 8.2 Applying Safeguards to the Programs Examined

SAFEGUARD \ SHARING DIRECTION	SNAP to Medicaid	Medicaid to SNAP	Medicaid to LTSS	LTSS to Medicaid
Data sharing agreement required	Yes	Yes	Yes	Yes
Field-level minimization applied	Recommended	Required (HIPAA minimum necessary)	Required (HIPAA minimum necessary)	Recommended
Purpose tagging enforced	Recommended	Required where PHI involved	Required where PHI involved	Recommended

IX. COMPOSITE ACCESS RISK MODELING

Access risk is not uniform across all users; it varies with both the privilege level a user holds and how frequently that privilege is exercised, a relationship that can be modeled as a composite risk surface.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

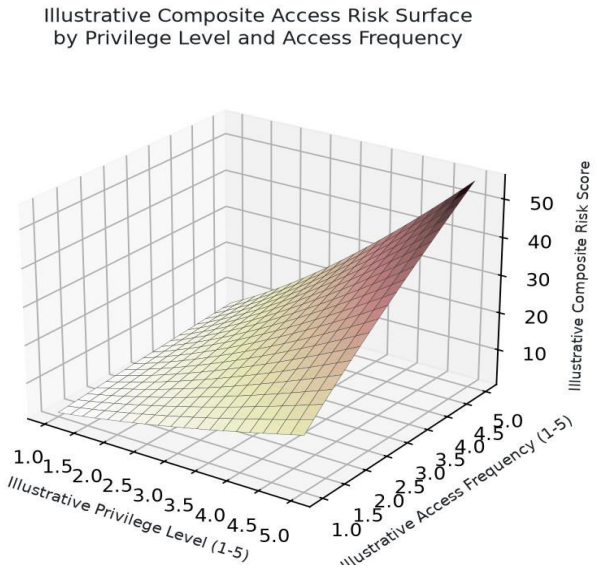


Figure 3. Illustrative composite access risk surface by privilege level and access frequency.

9.1 Interpreting the Risk Surface

As illustrated in Figure 3, composite risk rises non-linearly with privilege level, more steeply than with access frequency alone. This suggests that a small number of high-privilege accounts, even those accessed relatively infrequently, may carry greater composite risk than a larger number of lower-privilege accounts accessed frequently.

- **Highest risk zone:** Highest composite risk zone: accounts combining high privilege level with high access frequency, per the upper region of the surface in Figure 3, warranting the strongest combination of MFA, per Section 7.2, and access review, per Section 6.1.
- **Counterintuitive finding:** A privileged account accessed infrequently, such as a break-glass emergency access account, still carries meaningful composite risk under this model and should not be assumed low-risk simply due to infrequent use.

9.2 Applying the Risk Model to Governance Prioritization

Risk Zone	Illustrative Account Profile	Recommended Governance Priority
High privilege, high frequency	Active system administrators and data analysts with broad, routine access.	Highest priority for MFA, per Section 7.2, and frequent access review, per Section 6.1.
High privilege, low frequency	Break-glass emergency access accounts and infrequently used administrative accounts.	High priority for strong authentication and dormant access monitoring, per Section 6.1.
Low privilege, high frequency	Frontline caseworkers with routine, function-specific access.	Moderate priority; standard RBAC and periodic review per Sections 5 and 6 are generally sufficient.
Low privilege, low frequency	Occasional users with narrow, infrequent access needs.	Lower priority, though dormant access flagging per Section 6.1 remains relevant.

X. AUDITING AND MONITORING ACCESS TO PROTECTED INFORMATION

Auditing and monitoring provide the detection capability underlying every preventive control examined in prior sections, confirming that encryption and access control are functioning as designed in practice.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

10.1 Auditing and Monitoring Capability Comparison

Capability	Description	Cross-Program Consideration
Access logging	Recording every instance of data access, including user identity, timestamp, and data accessed.	Log formats should be standardized across programs to support the audit trail correlation described in Section 8.1.
Anomaly detection	Automated identification of access patterns deviating from established normal behavior.	Cross-program anomaly detection requires a shared baseline of normal behavior spanning program boundaries, not three separate, disconnected baselines.
Privileged access session recording	Detailed recording of privileged user sessions, including specific actions taken.	Particularly important for the highest composite risk zone identified in Section 9.2.
Regular audit log review	Scheduled, systematic review of audit logs, not solely automated alerting.	Should include specific review of cross-program access patterns, not only single-program review conducted independently by each program.

XI. THE FIVE STAGE SECURITY MATURITY MODEL

Programs can be classified into one of five maturity stages describing overall encryption and access control readiness, with maturity distribution varying by the scope of cross-program data sharing involved.

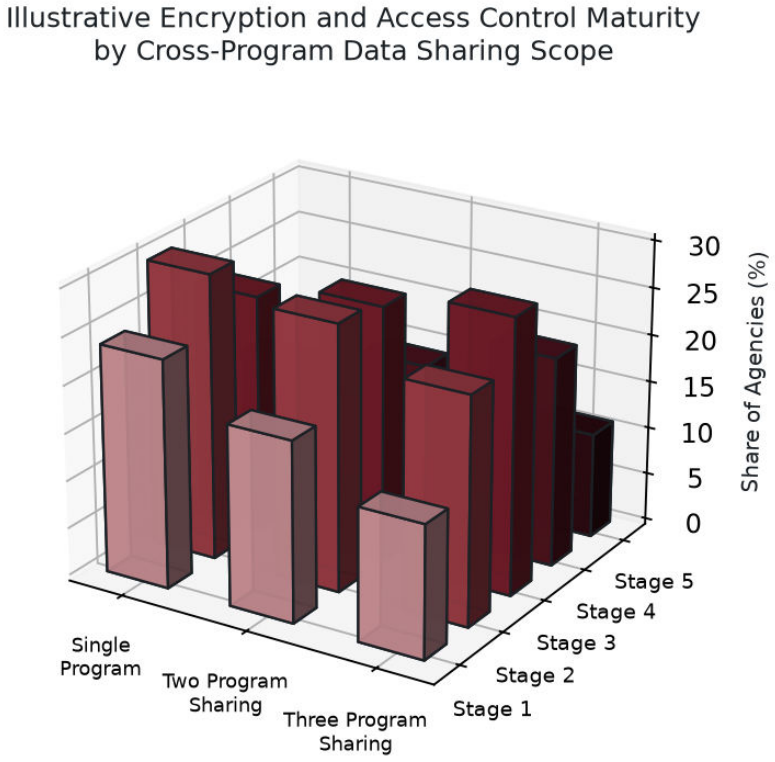


Figure 4. Illustrative encryption and access control maturity by cross-program data sharing scope.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Stage	Name	Description
1	Baseline	Basic encryption and access control exist but are not designed to the combined requirement principle in Section 2.2.
2	Aligned	Controls are aligned to the most stringent applicable requirement, per Section 2.2, but implementation is inconsistent across programs.
3	Standardized	Encryption architecture and RBAC design, per Sections 3 and 5, are applied consistently across all programs sharing data.
4	Governed	Cross-program data sharing safeguards, per Section 8, and auditing capability, per Section 10, operate under formal governance.
5	Risk-Adaptive	Composite access risk modeling, per Section 9, actively informs continuous, adaptive governance prioritization.

11.1 Maturity Distribution by Sharing Scope

As illustrated in Figure 4, programs sharing data across all three program areas show a maturity distribution shifted toward higher stages compared to single-program environments, consistent with the combined requirement principle in Section 2.2 forcing more deliberate security architecture design once cross-program sharing scope expands.

XII. GOVERNANCE STRUCTURES AND OWNERSHIP

Sustained encryption and access control effectiveness requires governance ownership spanning all three programs, distinct from any single program's independent security function.

12.1 Governance Roles

Role	Primary Responsibility	Governance Scope
Cross-program security architecture lead	Owns the encryption architecture and key management strategy described in Sections 3 and 4, designed to the combined requirement principle.	All three programs
Program-specific access control owner	Owns role definitions and access review for their specific program, per Sections 5 and 6.	Single program, coordinated across programs
Data sharing agreement steward	Owns the data sharing agreements and safeguards described in Section 8.	Cross-program data flows specifically
Security auditing and monitoring lead	Owns the auditing and monitoring capability described in Section 10, including cross-program audit correlation.	All three programs

12.2 Common Governance Gaps

- Program-specific access control owners occasionally design roles in isolation without confirming alignment to the combined requirement principle, reintroducing the compliance gaps the cross-program security architecture lead role is meant to prevent.
- Data sharing agreement stewardship is sometimes treated as a one-time legal or contracting activity rather than an ongoing governance function tracking actual data flows against agreed scope.

XIII. INCIDENT RESPONSE CONSIDERATIONS

Cross-program data sharing introduces incident response considerations beyond those relevant to a single program's independent incident response process.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

13.1 Cross-Program Incident Response Considerations

Consideration	Description	Recommended Approach
Multi-program breach notification coordination	A breach affecting shared data may trigger notification obligations under multiple programs' distinct requirements simultaneously.	Establish a coordinated notification process addressing all applicable program obligations rather than each program responding independently.
Cross-program forensic scope determination	Determining the full scope of a breach affecting shared infrastructure requires investigation across all programs sharing that infrastructure.	Ensure incident response plans explicitly address cross-program forensic coordination, not solely single-program scope.
Key compromise cross-program impact	A compromised encryption key under the hybrid key management approach in Section 4.1 may affect data across multiple programs.	Incorporate cross-program impact assessment into the event-driven key rotation practice described in Section 4.2.

XIV. RISK ASSESSMENT AND MITIGATION PLANNING

Cross-program encryption and access control programs carry risks that agencies should evaluate and mitigate deliberately, given the sensitivity of the protected health and benefits information involved.

Risk	Likelihood	Impact	Mitigation Approach
Encryption in use gap exploited during active processing	Moderate	High	Prioritize in-use encryption investment given the coverage gap identified in Section 3.2.
Cross-program role design misaligned with combined requirement principle	Moderate to High	High	Coordinate program-specific access control owners against the combined requirement principle (Section 12.2).
High composite risk accounts inadequately monitored	Moderate	High	Apply the risk-based governance prioritization in Section 9.2.
Data sharing agreement scope drift undetected	High	Moderate	Establish ongoing data sharing agreement stewardship as ongoing governance, not a one-time activity (Section 12.2).
Multi-program breach notification obligations missed or delayed	Moderate	High	Establish coordinated cross-program breach notification process per Section 13.1.

14.1 Risk Prioritization Guidance

- Cross-program role misalignment and multi-program breach notification risks should be treated as highest priority given their direct compliance and legal exposure.
- Encryption in use gaps and composite risk monitoring gaps are best addressed through the specific technical and governance investments identified in Sections 3.2 and 9.2 respectively.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

XV. IMPLEMENTATION ROADMAP

Translating this framework into an executable program requires sequencing regulatory alignment, encryption and access control design, and governance formation.

Phase	Approximate Timeframe	Key Milestones
Regulatory Alignment Assessment	Months 1 to 2	Confirm the combined requirement principle mapping per Section 2.2 across all shared data flows.
Encryption and Key Management Design	Months 2 to 6	Design encryption architecture per Section 3 and select a key management approach per Section 4.1.
RBAC and Access Review Implementation	Months 4 to 9	Implement cross-program RBAC design per Section 5 and establish access review cadence per Section 6.
Data Sharing Safeguards and Auditing	Months 7 to 11	Implement data sharing safeguards per Section 8 and cross-program auditing capability per Section 10.
Governance Formation and Continuous Operations	Months 10 onward	Establish governance roles per Section 12 and operate the KPIs described in Section 17.

🔒 15.1 Governance Cadence Reference

- **Monthly:** Review access review completion and dormant access flags per Section 6.1.
- **Quarterly:** Review cross-program audit correlation findings and data sharing agreement compliance per Sections 8 and 10.
- **Annually:** Conduct a full security maturity reassessment per Section 11.

XIV. CASE PATTERNS AND INDUSTRY BENCHMARKS

This article synthesizes recurring patterns observed across published HIPAA compliance and public sector data protection literature through early 2025, rather than reporting on a single named program.

Pattern Observed	Reported Association
Encryption architecture designed to the combined requirement principle from the outset	Fewer compliance gaps discovered during subsequent audit compared to programs layering protections independently (Section 2.2).
Hybrid key management with program-specific data encryption keys	Balanced cross-program access simplification against per-program key isolation risk (Section 4.1).
Cross-program role scoping with explicit assignment rather than inference	Reduced unintended cross-program access sprawl (Section 5.1).
Composite access risk modeling informing governance prioritization	More efficient allocation of limited security governance attention toward highest-risk accounts (Section 9.2).
Coordinated cross-program breach notification process established in advance	Faster, more complete breach notification compliance across all applicable program obligations (Section 13.1).

🔒 16.1 Cross-Program Observations

- **Observation 1:** Programs with a single, unified human services or health agency overseeing all three program areas reported faster alignment to the combined requirement principle than programs with fully separate program-specific agencies.
- **Observation 2:** Encryption in use remained the least mature capability across virtually all programs examined, reflecting broader industry-wide technical maturity limitations rather than a gap specific to human services programs.

© 2025 IJIRCCE | Volume 13, Issue 2, February 2025| DOI: 10.15680/IJIRCCE.2025.1302060

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

XVII. KEY PERFORMANCE INDICATORS FOR ONGOING GOVERNANCE

Sustaining encryption and access control value across SNAP, Medicaid, and LTSS requires an ongoing measurement framework spanning encryption coverage, access control maturity, and audit findings.

KPI	Definition	Illustrative Target
Encryption coverage by data state	Percentage of applicable systems and data covered by encryption, by state, benchmarked against Figure 1.	High and consistently increasing, particularly for in-use encryption.
Cross-program role alignment rate	Percentage of cross-program roles confirmed aligned to the combined requirement principle.	Full alignment across all cross-program roles.
Access review completion rate	Percentage of scheduled access reviews completed on time, per the cadence in Section 6.1.	High and consistent across all review types.
Composite risk zone coverage	Percentage of highest composite risk accounts, per Section 9.2, receiving the recommended governance priority controls.	Full coverage for the highest risk zone.
Data sharing agreement compliance rate	Percentage of actual data flows confirmed compliant with their governing data sharing agreement scope.	Full compliance across all active data flows.
Security maturity stage progression	Composite score tracked against the five stage model in Section 11.	Steady progression toward higher maturity stages.

SECURITY DESIGN NOTE

KPIs should be reviewed on the monthly, quarterly, and annual cadence described in Section 15.1, with particular attention to whether the highest composite risk zone identified in Section 9.2 consistently receives priority governance attention.

XVIII. CONCLUSION AND RECOMMENDATIONS

Encryption and access control for protected health and benefits information across SNAP, Medicaid, and LTSS systems must be designed to the combined, most stringent applicable requirement across all three programs, not the requirements of any single program considered independently. Agencies that design to this combined requirement principle from the outset report substantially fewer compliance gaps and materially stronger encryption and access control coverage than agencies layering protections onto independently designed program systems after the fact.

18.1 Summary of Key Findings

- Medicaid's HIPAA-driven requirements are consistently the most stringent among the three programs examined, meaning shared data and infrastructure should be designed to HIPAA Security Rule standards throughout.
- Encryption in use remains the least mature encryption capability across all three programs, representing the most significant remaining technical gap.
- Composite access risk rises non-linearly with privilege level, suggesting that a small number of high-privilege accounts may warrant disproportionate governance attention relative to their number.
- Cross-program data sharing safeguards, including data sharing agreements, field-level minimization, and purpose-based access tagging, address risks that encryption and access control alone do not fully mitigate.

18.2 Recommendations

- **Recommendation 1:** Design encryption and access control architecture to the combined requirement principle from the outset of any cross-program data sharing initiative.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Recommendation 2:** Prioritize in-use encryption investment given its consistently low illustrative coverage across all three programs examined.
- **Recommendation 3:** Apply composite access risk modeling, per Section 9, to prioritize limited security governance attention toward the highest-risk accounts rather than applying uniform effort across all accounts.
- **Recommendation 4:** Establish cross-program governance roles, per Section 12, with explicit accountability spanning all three programs rather than relying on independent, program-specific security functions alone.

REFERENCES

[1] U.S. Department of Health and Human Services, Office for Civil Rights. (2013). "HIPAA Security Rule," 45 CFR Part 160 and Part 164, Subparts A and C.
[2] U.S. Department of Health and Human Services, Office for Civil Rights. (2009, updated 2013). "HIPAA Breach Notification Rule," 45 CFR 164.400-414.
[3] U.S. Department of Health and Human Services, Office for Civil Rights. (2003, updated 2013). "HIPAA Privacy Rule," 45 CFR Part 160 and Part 164, Subparts A and E.
[4] Centers for Medicare and Medicaid Services (CMS). (2015). "Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0." CMS Technical Guidance.
[5] National Institute of Standards and Technology (NIST). (2020). "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53, Revision 5.
[6] National Institute of Standards and Technology (NIST). (2019). "Attribute Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162.
[7] National Institute of Standards and Technology (NIST). (2020). "Digital Identity Guidelines," NIST Special Publication 800-63-3.
[8] National Institute of Standards and Technology (NIST). (2020). "Recommendation for Key Management," NIST Special Publication 800-57 Part 1, Revision 5.
[9] National Institute of Standards and Technology (NIST). (2001, with subsequent updates). "Advanced Encryption Standard (AES)," FIPS Publication 197.
[10] Ferraiolo, D.F., Kuhn, D.R., & Chandramouli, R. (2007). "Role-Based Access Control," 2nd Edition. Artech House.
[11] U.S. Government Accountability Office. (2019). "Cybersecurity: Governance and Reporting Practices at Federal Agencies." GAO-19-336.
[12] U.S. Government Accountability Office. (2021). "Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Face Challenges." GAO Report.
[13] National Association of State Chief Information Officers (NASCIO). (2022). "State Identity and Access Management Governance Practices." NASCIO Research Brief.
[14] American Public Human Services Association (APHSA). (2021). "Shared Services Identity Management Across Human Services Agencies." APHSA Policy Brief.
[15] Urban Institute. (2019). "Integrated Eligibility Systems and Cross Program Enrollment: A Fifty State Review." Urban Institute Research Report.
[16] Kaiser Family Foundation. (2019). "Medicaid Eligibility and Enrollment Systems Modernization: State Trends." KFF Issue Brief.
[17] Health Level Seven International (HL7). (2019). "Fast Healthcare Interoperability Resources (FHIR), Release 4." HL7 Standard Specification.
[18] Cloud Security Alliance (CSA). (2020). "Cloud Controls Matrix, Version 4." CSA Publication.
[19] SANS Institute. (2020). "Critical Security Controls for Effective Cyber Defense." SANS Whitepaper.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details